UNIVERSIDAD MIGUEL HERNÁNDEZ

FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS DE ELCHE

GRADO EN RELACIONES LABORALES Y RECURSOS HUMANOS

TRABAJO DE FIN DE GRADO

EL CONTROL EMPRESARIAL A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS: UN ESTUDIO DE SU LICITUD

CURSO ACADÉMICO 2018/2019

ALUMNA: LAURA ESPINOSA ABELLÁN

TUTORA: DRA. PALOMA ARRABAL PLATERO

ÍNDICE

ABREVIATURAS

AEPD	Agencia Española de protección de Datos
AN	Audiencia Nacional
ATS	Auto del Tribunal Supremo
CE	Constitución Española, de 27 de diciembre de 1978
CEDH	Convenio Europeo de Derechos Humanos
DDFF	Derechos Fundamentales
ET	Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
FJ	Fundamento Jurídico
GPS	Dispositivo de Posicionamiento Global (*Global Positioning System*)
LEC	Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LOPJ	Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
LRJS	Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social.
LSP	Ley 5/2014, de 4 de abril, de Seguridad Privada
NTIC	Nuevas Tecnologías de la Información y de la Comunicación
Núm.	Número
Pág.	Página
Rec.	Recurso

RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE
RRLL	Relaciones Laborales
RSP	Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STS	Sentencia del Tribunal Supremo
STSJ	Sentencia del Tribunal Superior de Justicia
TEDH	Tribunal Europeo de Derechos Humanos
TC	Tribunal Constitucional
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia

RESUMEN

El presente trabajo tiene por objeto analizar la problemática que gira en torno a la confrontación entre los DDFF de los trabajadores y el poder de control empresarial. Este conflicto, lejos de ser nuevo, queda totalmente renovado con la incursión de las nuevas tecnologías en el ámbito laboral.

Los tribunales han sido los encargados de trazar las líneas maestras respecto del uso de dispositivos digitales como herramientas de vigilancia y de trabajo, debido a la falta de normativa que existía en este sentido. Con la reciente entrada en vigor de la LOPDGDD, el legislador ha tratado de aportar soluciones a esta incógnita. No obstante, la interpretación de los tribunales continúa siendo necesaria, pues la nueva normativa resulta insuficiente.

Este trabajo se centra en estudiar qué condiciones debe cumplir la actuación empresarial para afirmar que, desde un punto de vista procesal, su uso no lesiona ningún derecho fundamental. Para ello, se analizan diferentes modalidades de vigilancia de los trabajadores, esto es, el control audiovisual, la monitorización del ordenador como herramienta de trabajo, la geolocalización y el control biométrico.

INTRODUCCIÓN

La expansión de las nuevas tecnologías ha tenido un gran impacto en todos los ámbitos de la sociedad, revolucionando profundamente la forma en que hablamos, nos relacionamos e, incluso, trabajamos. Este nuevo modelo de sociedad ha traído consigo la necesidad de consumir información como un producto más, convirtiendo Internet en un bien imprescindible para cualquier ciudadano.

En los últimos años, el uso de dispositivos tecnológicos con acceso a internet se ha intensificado en nuestro día a día, llegando a generar nuevos conflictos en torno a la perdurabilidad de nuestros datos en la red o las patologías relacionadas con el uso abusivo del teléfono móvil[1].

Las organizaciones empresariales no han sido ajenas a esta transformación, viéndose claramente influenciadas por el desarrollo informático[2]. En este sentido, la aplicación de las NTIC al mundo empresarial ha resultado un factor clave para el nacimiento de nuevas figuras laborales a través de modelos económicos alternativos. Sirva de ejemplo plataformas digitales de reparto a domicilio como Glovo o Deliveroo, o las aplicaciones de economía colaborativa Badi o AirBnB, donde los usuarios intercambian su vivienda[3].

Del mismo modo, esta generalización tecnológica ha contribuido al desarrollo de nuevos modos de trabajo (piénsese en el teletrabajo), así como nuevas formas de vigilancia de los trabajadores (véase la videovigilancia). La informática permite al

[1] Véase en este sentido la noticia sobre la nomofobia (ansiedad y miedo que provoca no disponer de un teléfono móvil), elaborada por "Efesalud", plataforma digital de la Agencia Efe especializada en contenidos de salud. Disponible en: https://www.efesalud.com/nomofobia-esclavos-del-movil/ (última visita: 16/07/2019). Según el "Informe ditrendia: Mobile en España y en el Mundo 2018", "el móvil es el dispositivo más utilizado en España para acceder a internet, usado ya por el 97% de los españoles", elaborado por Ditrendia. Disponible en: https://mktefa.ditrendia.es/hubfs/Ditrendia-Informe%20Mobile%202018.pdf?t=1532079210754&utm_campaign=Informe%20Mobile%202018&utm_source=hs_automation&utm_medium=email&utm_content=64334773&_hsenc=p2ANqtz--cx3JSF8KsY23QL5n_hdEfexpA53INssRdwpW2vGb0GDM4dsTbTyo (última visita 16/07/2019).

[2] La "Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del comercio electrónico en las empresas", elaborada por el Instituto Nacional de Estadística (INE), recoge que "tres de cada cinco empleados en empresas con diez o más trabajadores usan ordenadores con fines empresariales y más de la mitad utiliza ordenadores con conexión a Internet en el primer trimestre de 2018". Asimismo, expone que el 79,80% de las empresas españolas con menos de diez empleados dispone de ordenadores, mientras que el 75,54% tienen acceso a internet. En cuanto a las empresas con más de diez trabajadores, el 99,22% cuenta con ordenadores, y el 98,65% dispone de acceso a internet. Disponible en: https://www.ine.es/prensa/tic_e_2017_2018.pdf (última visita: 16/07/2019).

[3] Véase en este sentido la ponencia "Las prestaciones de servicios a través de las plataformas digitales: un nuevo desafío para el Derecho del Trabajo" impartida por CAVAS MARTÍNEZ, F., en el marco del III Seminario del área de Derecho del Trabajo y de la Seguridad Social, celebrado el 1 de marzo de 2017 en la Universidad Miguel Hernández de Elche (Alicante). Disponible en: https://youtu.be/RK1-B1yd5gs (última visita: 18/07/2019).

empresario utilizar los mecanismos de control con una mayor eficacia y comodidad, facultándole de un poder que, lejos de ser ilimitado, puede resultar muy intrusivo para la intimidad del trabajador. En consecuencia, gran parte de los actuales conflictos laborales surgen de la confrontación entre la vigilancia electrónica de los trabajadores y los DDFF[4].

Asimismo, el avance tecnológico también ha alcanzado al ámbito procesal permitiendo el nacimiento de las llamadas "pruebas tecnológicas" y haciendo cada vez más usual el empleo de medios de prueba consistentes en correos electrónicos, mensajería instantánea o publicaciones en redes sociales, en los procesos judiciales[5].

En este contexto, recientemente han entrado en vigor dos normativas en materia de protección de datos: por un lado, el RGPD, cuyo fin es unificar toda la legislación existente en la UE; y por otro, la LOPDGDD, que entra a regular de manera específica el uso de los dispositivos tecnológicos en el ámbito de las RRLL en España. En consecuencia, actualmente vivimos una etapa de adaptación normativa, por lo que están siendo los tribunales los encargados de resolver los conflictos en este sentido.

Sobre la base de las ideas expuestas, el presente trabajo se estructura en dos epígrafes: el primero, analiza las facultades que la ley confiere al empresario en virtud de su posición de empleador, así como sus limitaciones; el segundo, aborda distintos tipos de medios tecnológicos de control a través de los cuales el empresario puede ejercer su poder de control.

De este modo, el primer epígrafe comienza con un estudio de los poderes del empresario, centrándose en la facultad de control sobre la actividad laboral. Seguidamente, el trabajo continúa analizando las limitaciones que el empresario encuentra en cuanto a su capacidad de vigilancia, esto es, la dignidad del trabajador, los DDFF y la licitud de las pruebas obtenidas con ocasión de la medida aplicada.

Por su parte, el segundo epígrafe aborda distintos tipos de medios tecnológicos de control a través de los cuales el empresario puede ejercer su poder de control. Concretamente, se analiza la jurisprudencia y la doctrina en este sentido, con el fin de

[4] Véase en este sentido el artículo "Las consecuencias laborales y sociales del avance de las nuevas tecnologías en el mundo empresarial", del blog del bufete de abogados Casadeley. Disponible en: https://www.bufetecasadeley.com/consecuencias-laborales-tecnologia-empresas/ (última visita: 20/07/2019).

[5] El artículo "La prueba digital en el procedimiento laboral" expone que "desde hace algunos años, en el ámbito del procedimiento laboral, es más que habitual la aportación de pruebas de origen "digital" o "electrónico", publicado por el abogado Pere Vidal López en el Blog Laboral de LegalToday. Disponible en: http://www.legaltoday.com/practica-juridica/social-laboral/laboral/la-prueba-digital-en-el-procedimiento-laboral (última visita: 22/07/2019).

dilucidar qué condiciones son las necesarias para que el empresario ejerza su poder de control de forma legítima.

En definitiva, este trabajo realiza una aproximación a los medios de control a los que los trabajadores se ven sometidos con ocasión de las nuevas tecnologías, estudiando cómo se resuelve esta problemática y analizando qué condiciones debe cumplir la actuación empresarial para afirmar que su uso no lesiona ningún derecho fundamental.

EPÍGRAFE I.- EL CONTROL EMPRESARIAL SOBRE LA ACTIVIDAD LABORAL

1.- LOS PODERES DEL EMPRESARIO: DIRECCIÓN, CONTROL Y DISCIPLINA

En virtud de la normativa aplicable, todos los trabajadores ostentan una serie de derechos y deberes que se adquieren como consecuencia del vínculo contractual establecido con un empleador. Así, a través del contrato de trabajo, el empleado queda obligado a cumplir con un conjunto de obligaciones básicas como son, entre otras, el deber de obediencia y disciplina, el deber de buena fe y el deber de diligencia. Esto supone que la prestación o servicio pactado debe realizarse siguiendo las órdenes e instrucciones del empresario (o persona en la que este delegue para tal circunstancia), observando para ello las normas de buena fe y actuando con la diligencia debida[6].

Como contrapartida a estas obligaciones, el empresario posee un conjunto de poderes que buscan organizar la actividad laboral con el propósito final de aumentar sus beneficios[7]. Estos poderes, encuentran actualmente su fundamento jurídico en la Constitución Española (en adelante, CE) como marco general, siendo después desarrollados de una forma más completa por el Estatuto de los Trabajadores (en adelante, ET)[8].

El artículo 38 CE reconoce el derecho a la libertad de empresa por el que todo ciudadano goza de la potestad para crear su propio negocio. Este precepto, a pesar de no reconocer los poderes del empresario de una forma directa, ha sido ampliado por consolidada jurisprudencia al respecto, concluyendo que el empresario también posee una libertad de organización y dirección de la actividad laboral que ejerce en atención a sus propias necesidades[9].

---

[6] El artículo 5 ET sobre deberes laborales expresa que "los trabajadores tienen como deberes básicos: a) cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia; b) observar las medidas de prevención de riesgos laborales que se adopten; c) cumplir las órdenes e instrucciones del empresario en el ejercicio regular de sus facultades directivas; d) No concurrir con la actividad de la empresa, en los términos fijados en esta ley; e) contribuir a la mejora de la productividad; f) cuantos se deriven, en su caso, de los respectivos contratos de trabajo".

[7] En este sentido, la autora LLAMOSAS TRAPAGA expresa que "se reconoce al empresario el derecho a constituir la coyuntura necesaria para la producción de bienes con el fin de ofrecerlos al mercado y de esa forma tratar de obtener una serie de beneficios (…) y por ello resulta sensato pensar en que debe atribuírsele ese poder de control y disciplinario para verificar la buena marcha de la empresa", en *Relaciones laborales y nuevas tecnologías de la información y de la comunicación*, Dykinson, Madrid, 2015, pág. 118.

[8] Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

[9] Véanse en este sentido las SSTC 96/2013, de 23 de abril; 96/2002, de 25 de abril; y 225/1993, de 8 de julio.

En este mismo sentido, el ET otorga al empresario tres facultades. Estas son: el poder de dirección, el poder de control y el poder disciplinario; que serán tratadas a continuación.

Así, el artículo 20 ET atribuye al empleador una potestad que nace con ocasión de un contrato de trabajo y que se concreta a través de los poderes de dirección y de control[10]. En primer lugar, podemos definir el poder de dirección como la facultad empresarial de organizar, a través de órdenes e instrucciones, la actividad laboral y, por ende, a los trabajadores[11]. En cuanto al poder de control, este implica la capacidad de vigilar a los empleados con el fin de verificar la efectiva prestación de sus servicios adoptando para ello las medidas que considere más apropiadas[12].

Por su parte, el artículo 58 ET otorga al empresario una potestad disciplinaria cuya finalidad es imponer la eventual sanción a aquellos empleados que no cumplan con las obligaciones previamente establecidas. Esta facultad sirve como garantía para el efectivo cumplimiento de los poderes de dirección y control, pues se configura como una importante herramienta del empresario con la que lograr su objetivo final, esto es, obtener beneficios[13].

No obstante todo lo expuesto, el empresario no cuenta con una absoluta libertad para ejercer estos poderes, sino que existen ciertas limitaciones impuestas por el ordenamiento jurídico como el respeto a los Derechos Fundamentales (en adelante, DDFF), como veremos[14].

---

[10] En cuanto al poder de dirección y control, el artículo 20 ET, dispone que "el trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien este delegue (…) el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad."

[11] Afirma MONTOYA MELGAR que "el poder de dirección del empresario tiene una doble dimensión: general (como poder de organizar laboralmente la empresa) y singular (como poder de ordenar las concretas prestaciones de los trabajadores individuales) (…) del que se ocupa el Estatuto de los Trabajadores…", en "El poder de dirección del empresario en las estructuras empresariales complejas", *Revista del Ministerio de Trabajo y Asuntos Exteriores*, núm. 48, 2004, págs. 135-136.

[12] Según MONTOYA MELGAR, "la vigilancia es un aspecto del poder de dirección con el que se encuentra en relación de parte a todo; se refiere al control fiscalizador que el empresario ejerce sobre el cumplimiento de la prestación laboral, y es el necesario complemento de la potestad ordenadora del empresario", "Dirección y control de la actividad laboral (artículo 20 ET)", *Comentarios a leyes laborales. Estatuto de los trabajadores* (Dir. BORRAJO DACRUZ, E.), Tomo V, Edersa, Madrid, 1985, pág. 143.

[13] LLAMOSAS TRAPAGA, A., *Relaciones laborales y nuevas… Op. Cit.*, pág. 119.

[14] Según GOÑI SEIN, los DDFF son los recogidos en la Sección primera del Capítulo II del Título primero de la CE (artículos 15 al 29 CE), junto con los artículos referidos a la igualdad (artículo 14 CE) y a la objeción de conciencia (artículo 30 CE), en "Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?", *XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, Ediciones Cinca, 2014, pág. 10.

La práctica de los poderes del empresario ha evolucionado con el paso del tiempo gracias, en gran medida, a la aplicación de las nuevas tecnologías de la información y de la comunicación (en adelante, NTIC) al ámbito laboral[15]. Esto ha supuesto una gran revolución tanto en las formas de trabajar de los empleados, como en los instrumentos de dirección y control empresarial, permitiendo así, desarrollar su trabajo y ejercer sus derechos de una manera diferente.

Asimismo, este uso de herramientas informáticas en las organizaciones ha originado dos efectos muy importantes: por un lado, se ha incrementado la autonomía de la que disponen los trabajadores durante el ejercicio de su actividad laboral generando así nuevas formas de trabajar[16]; por el otro, el empresario ha desarrollado modos de supervisión y control más intensos y difíciles de apreciar para los trabajadores[17].

Dichos cambios organizativos han favorecido el surgimiento de una serie de conflictos en tanto en cuanto la utilización de las NTIC implica una mayor confusión entre la esfera de la vida privada y la esfera de lo profesional de los trabajadores, llegando a superponerse en ciertos aspectos[18].

Esta problemática se hace patente en la aplicación de medios tecnológicos en el ámbito laboral como son los sistemas de geolocalización (en adelante, GPS)[19]. El GPS es una herramienta que permite conocer la ubicación de un dispositivo en todo momento, por lo que su uso como herramienta de control faculta al empleador a realizar un seguimiento exhaustivo de los desplazamientos que realiza un trabajador. Así, el acceso

---

[15] Véase en este sentido la "Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del comercio electrónico en las empresas", elaborada por el Instituto Nacional de Estadística (INE), donde se recoge que "tres de cada cinco empleados en empresas con diez o más trabajadores usan ordenadores con fines empresariales y más de la mitad utiliza ordenadores con conexión a Internet en el primer trimestre de 2018" y que el uso de medios sociales por las empresas (con conexión a internet) asciende al 51,8%, según datos relativos al primer trimestre de 2018. Disponible en: https://www.ine.es/prensa/tic_e_2017_2018.pdf (última visita: 20/03/2019).

[16] LÓPEZ PEÑA, A., *Innovación tecnológica y cualificación (La polarización de las cualificaciones de la empresa)*, CES, Madrid, 1996, pág. 32.

[17] PUJOLAR, O. "Poder de dirección del empresario y nuevas formas de organización y gestión del trabajo", *Relaciones Laborales: Revista crítica de teoría y práctica*, 2005, núm. 2, pág. 6.

[18] En este sentido, la STC 88/1985, de 19 de julio, establece que las organizaciones empresariales no se presentan como "mundos separados y estancos del resto de la sociedad", por lo que la libertad de empresa que ostentan no puede limitar injustificadamente los DDFF de los trabajadores asalariados. Del mismo modo se manifiesta ARRABAL PLATERO cuando dice que "los nuevos métodos tecnológicos permiten al empleador mayor control y vigilancia sobre sus empleados, un control que no tiene sus límites bien definidos (…) Así, un problema que ha existido siempre se configura de manera diversa por los nuevos instrumentos de control que se encuentran ahora a disposición de los empleadores", en su artículo "La videovigilancia laboral como prueba en el proceso", *Revista General de Derecho Procesal IUSTEL*, núm. 37, 2015, pág. 4.

[19] LLAMOSAS TRAPAGA afirma que "la localización de los trabajadores a través de medios telemáticos" (…) "se halla estrechamente vinculada al uso intensivo de las nuevas tecnologías dentro del ámbito del Derecho del Trabajo", en *Relaciones laborales y nuevas… Op. Cit.*, pág. 27.

del empresario a tal cantidad de datos ha propiciado la necesidad de trazar las líneas que separan el ejercicio legítimo del poder de control, de la intromisión ilegítima del empresario en la intimidad de los trabajadores[20].

En este sentido se pronuncia el Tribunal Constitucional (en adelante, TC) cuando expresa: "Los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las comunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental que extienda la protección de estos nuevos ámbitos"[21].

Se evidencia, por tanto, la necesidad de determinar qué derechos y obligaciones entran en juego en relación con el uso de los medios tecnológicos en el ámbito laboral.

2.- LOS LÍMITES AL EJERCICIO DEL PODER DE CONTROL EMPRESARIAL

Como se ha mencionado, el empresario posee la potestad de establecer las medidas de vigilancia que considere, con el fin de ejercer su derecho de control. Sin embargo, este poder no es absoluto, y no toda medida resulta lícita. Por lo que se hace necesario establecer un equilibrio entre los intereses empresariales y los derechos de los trabajadores.

Así, encontramos en los DDFF un primer límite al ejercicio del poder empresarial[22]. Estos, son derechos a los que la CE otorga un valor especial (de ahí su nombre) y que asisten a todos los ciudadanos. Por tanto, en la medida en que los ciudadanos pueden ejercitar su derecho al trabajo, los DDFF también operarán en el marco de las relaciones laborales (en adelante, RRLL), puesto que la existencia de un vínculo contractual no

[20] Véase la entrada "Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral" publicada por la abogada Alexandra Garcés en el blog de la firma ECIJA. Disponible en: https://ecija.com/derecho-a-la-intimidad-ante-la-utilizacion-de-sistemas-de-geolocalizacion-en-el-ambito-laboral/ (última visita: 12/04/2019).

[21] STC 70/2002, de 3 de abril, FJ 9º.

[22] ROMÁN DE LA TORRE expresa que "el primer criterio es el de que los derechos fundamentales del trabajador han de encontrar su ámbito de ejercicio y respeto en la relación de trabajo y, lo que es más importante por lo que a nuestro tema se refiere, esos derechos, integrados en el modelo laboral del que se parte, limitan el ejercicio de los poderes empresariales y la propia concepción intrínseca de éstos, al no poder ser concebidos de una forma absoluta, independientemente del juego de limites recíprocos que tendrán entre sí tales derechos", en *Poder de dirección y contrato de trabajo*, Grapheus, Valladolid, 1993, págs. 301-302.

supone la restricción de derechos constitucionales para ninguna de las partes[23]. En otras palabras, existe una serie de DDFF que pueden ser ejercidos en el ámbito de una prestación laboral.

Al igual que ocurre con el poder de control empresarial, los DDFF tampoco son absolutos, pues admiten ciertas limitaciones de índole organizativa y/o productiva, siempre y cuando estas sean indispensables y necesarias en atención al interés empresarial[24]. Estos derechos son[25]: el derecho a la igualdad y a la no discriminación; el derecho a la libertad ideológica y religiosa; el derecho al honor, a la intimidad personal y a la propia imagen; el derecho al secreto de las comunicaciones, el derecho a la protección de datos de carácter personal; el derecho a la libertad de expresión; el derecho a la libertad de información; el derecho de reunión; el derecho a la tutela judicial efectiva; el derecho a la aplicación del principio de legalidad; y derecho a la educación[26].

De igual forma, el ordenamiento laboral fija un conjunto de deberes empresariales que también vienen a restringir el poder de vigilancia y control del empresario[27]. En este sentido, el artículo 20.3 ET impone al empleador la necesidad de respetar la dignidad del trabajador en lo concerniente a las medidas de vigilancia y control aplicadas. Esta dignidad "obliga a reconocer a cualquier persona, independientemente de la situación en que se encuentre, aquellos derechos o contenidos de los mismos imprescindibles para garantizarla", según enuncia el TC[28].

---

[23] Tal y como indica la STC 88/1985, de 19 de julio, "la celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le concede como ciudadano". En este mismo sentido se pronuncia GOÑI SEIN cuando expresa que estos DDFF "se convierten en verdaderos derechos laborales cuando se hacen valer en el marco de la relación laboral", en su obra "Los derechos fundamentales inespecíficos en…", *Op. Cit*., pág. 21.

[24] Así lo explica CAVAS MARTÍNEZ, F., en su ponencia "Los Derechos y Libertades Fundamentales en materia laboral", realizada en el marco del I Seminario del Área de Derecho del Trabajo y la Seguridad Social y que tuvo lugar el 23 de febrero de 2015 en la Universidad Miguel Hernández de Elche (Alicante). Disponible en: https://www.youtube.com/watch?v=fECK5u0FO6A (última visita: 15/03/2019). Véanse en este sentido las SSTC 98/2000, de 10 de abril; 143/1994, de 9 de mayo; y 57/1994, de 28 de febrero.

[25] PALOMEQUE LÓPEZ denomina a los DDFF ejercidos en el contexto de una relación laboral "derechos constitucionales laborales inespecíficos" definiéndolos como "derechos atribuidos con carácter general a los ciudadanos, que son ejercitados en el seno de una relación jurídica laboral por ciudadanos que, al propio tiempo, son trabajadores y, por lo tanto, se convierten en verdaderos derechos laborales por razón del sujeto y de la naturaleza de la relación jurídica en que se hacen valer, en derechos constitucionales laborales inespecíficos", en *Los derechos laborales en la Constitución Española*, CES, Madrid, 1991, pág. 31.

[26] Véase la entrada "La Constitución Española y su contenido laboral" del blog del profesor FERNÁNDEZ GARCÍA. Disponible en: https://aflabor.wordpress.com/2012/12/11/la-constitucion-espanola-y-su-contenido-laboral/ (última visita: 06/04/2019).

[27] Además, el artículo 64.5.f) ET también contempla como una de las competencias del Comité de Empresa la de ser informado y consultado sobre las decisiones adoptadas por la empresa, así como la emisión de informes previos a la ejecución de la decisión del empresario. También la normativa sobre prevención de riesgos laborales expresa la necesidad de respeto a la intimidad de los trabajadores que deben guardar las medidas de vigilancia y control de la salud de los trabajadores.

[28] STC 236/2007, de 7 de noviembre.

Por otro lado, las dos partes de una relación laboral están sometidas al principio de la buena fe contractual, según el cual, ambos se obligan a actuar con una fidelidad mutua en el ejercicio de sus prestaciones[29]. El quebrantamiento de este deber de buena fe aparece en el ET constituyéndose como una de las causas del despido disciplinario, pues se trata de un incumplimiento contractual en virtud del cual el empresario puede decidir unilateralmente la extinción la relación laboral[30].

Resulta relevante apuntar que el ordenamiento jurídico no ofrece un concepto claro de lo que se entiende por buena fe, por lo que es necesario acudir a la jurisprudencia que, atendiendo a cada caso concreto, dicta si una acción constituye -o no- una transgresión.

En este sentido, el Tribunal Supremo (en adelante, TS) ha venido interpretando como buena fe contractual el "criterio objetivo, constituido por una serie de pautas coherentes con el comportamiento en las relaciones humanas y negociales, que en materia contractual no solo funciona como un canon hermenéutico de la voluntad reflejada en el consentimiento, sino también como una fuente de integración del contenido normativo del contrato, que actúa por vía dispositiva, a falta de pacto y abstracción hecha de la intención o de la voluntad de las partes, de tal forma que estas consecuencias que complementan el contrato haya su fundamento vinculante no solo en el mismo, en sus indicaciones explícitas o implícitas, sino en la norma o principio general de la buena fe"[31].

Esta misma falta de claridad normativa sufría el uso de las NTIC en el ámbito laboral, hecho que resulta sorprendente si tenemos en cuenta el contexto digital que viven las organizaciones desde tiempo atrás. No obstante, la reciente publicación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD)[32] ha incluido diversos preceptos relativos al derecho a la desconexión digital de los trabajadores, a la protección de la intimidad en el uso de las NTIC, y frente al control empresarial ejercido a través de la videovigilancia, la geolocalización y la grabación de sonidos[33].

[29] Véase en este sentido la STSJ Cataluña 8041/2001, de 22 de octubre, donde se expresa que tanto el trabajador como el empleador deben someterse, de manera recíproca, a las exigencias de la buena fe contractual en el desarrollo de sus prestaciones.

[30] El artículo 54.2 ET sobre el despido disciplinario expone que "se considerarán incumplimientos contractuales (…) d) La transgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo". Por otra parte, el artículo 7.1 del Código Civil dispone que "los derechos deberán ejercitarse conforme a las exigencias de la buena fe".

[31] STS 479/2009, de 15 de junio.

[32] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[33] Véanse los artículos 87 - 91 LOPDGDD.

De igual forma, se incorpora al ET el artículo 20.bis sobre los "derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión"[34].

Con todo, la determinación del alcance del poder de control empresarial en atención al uso de las NTIC sigue resultando materia de controversia, pues esta facultad puede contravenir el ejercicio de los DDFF de los trabajadores[35]. Derechos que no podrán transgredirse, si bien, podrán resultar limitados como consecuencia de la confrontación con los intereses de terceros.

2.1.- Los Derechos Fundamentales como límite al control empresarial

Tal y como se ha avanzado, los DDFF se configuran como una garantía constitucional que protege el ejercicio de los derechos y libertades que poseen los trabajadores en el marco de las RRLL. Ahora bien, los DDFF también sirven de límite a los poderes que ostenta el empresario, puesto que el control empresarial puede constituir una vulneración de los derechos de los trabajadores, en la medida en que su práctica sea ilegítima.

A este respecto, en el contexto de los conflictos laborales derivados del uso de NTIC, cobran especial relevancia los DDFF relativos a la intimidad, al secreto de las comunicaciones y a la protección de datos de carácter personal, todos ellos contenidos en el artículo 18 CE[36]. Estos, son derechos estrechamente vinculados entre sí que se caracterizan por ser personalísimos (solo las personas físicas pueden invocarlo y se extingue con el fallecimiento del individuo) e irrenunciables. Sin embargo, esta conexión no significa que no gocen de autonomía, pues contienen importantes rasgos diferenciadores, como veremos.

[34] Este artículo se añade por la disposición adicional 13 LOPDGDD y declara que "Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

[35] Véase en este sentido la STC 88/1985, de 19 de julio, que niega que el derecho a la libertad de empresa permita la limitación injustificada de los DDFF de los trabajadores.

[36] El artículo 18 CE expresa que: "1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.; 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.; 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.; 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

2.1.1.- El Derecho Fundamental a la intimidad personal y familiar

El artículo 18.1 CE reconoce el derecho a la intimidad personal y familiar de todos los ciudadanos con el fin de garantizar "el secreto sobre la propia esfera de la vida personal, prohibiendo a los terceros, particulares o poderes públicos, decidir sobre los contornos de la vida privada", según interpreta el TC[37]. Este derecho, también se encuentra reconocido en el artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales (en adelante, CEDH)[38], así como en la Ley de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen[39].

La garantía de la intimidad supone el disfrute de la privacidad a través del control de la información personal y familiar existente, así como la oposición del ciudadano a que determinados aspectos de su vida privada (como la intimidad corporal, la salud, la vida sexual, o circunstancias relativas a terceros que puedan incidir en el desarrollo del individuo) sean utilizados para fines distintos de aquel que, siendo legítimo, justificó la obtención de los datos[40].

Por su parte, el ET también hace alusión a la intimidad cuando establece como derechos laborales básicos el respeto a la intimidad del trabajador y la garantía de la inviolabilidad de su persona, entre otros[41]. Esta garantía choca con la potestad que tiene el empresario para realizar registros de los trabajadores, sus taquillas y/o efectos personales (siempre y cuando el patrimonio empresarial o del resto de empleados se encuentre en peligro)[42]. Dichos registros, deben tener lugar dentro del espacio y horario laboral, y con la presencia del trabajador en cuestión y/o de su representante legal, o, en su defecto, otro trabajador[43]. Además, como ya se ha mencionado en párrafos anteriores,

[37] Así ha interpretado el TC el artículo 18.1 CE en la sentencia 70/2009, de 23 de marzo.
[38] Convenio para la protección de los derechos humanos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950 (ratificado por España el 4 de octubre de 1979).
[39] Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
[40] Así lo enuncia la STC 134/1999, de 15 de julio, cuando describe la intimidad personal y familiar como el derecho a "tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia". En el mismo sentido, la STC 186/2000, de 10 de julio, hace referencia a la intimidad personal y familiar como "núcleo central de la personalidad", lo que implica una "facultad de exclusión de los demás". Véase también el FJ 2º de la STC 202/1999, de 8 de noviembre.
[41] Véanse los artículos 4.2.e) y18 ET.
[42] Según la STS, de 11 de junio de 1990, el vehículo particular del trabajador también se considera un efecto personal, por lo que puede ser registrado si se encuentra dentro del recinto de la empresa.
[43] ARIAS DOMÍNGUEZ, y RUBIO SÁNCHEZ establecen que el "lugar de trabajo" comprende la zona de aparcamiento, de almacenaje, jardines y los servicios comunes de la empresa como calles y plazas interiores. En *El derecho de los trabajadores a la intimidad*, Aranzadi, Pamplona, 2006, pág. 80.

recientemente ha sido incorporado al ET el artículo 20.bis, referente al uso de NTIC en el ámbito laboral. Este precepto establece que todo trabajador tiene los siguientes derechos: a la intimidad en el uso de las herramientas informáticas que el empresario le proporciona; a la desconexión digital fuera de su horario laboral; y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización conforme a la normativa en materia de protección de datos personales[44].

En este punto, resulta fundamental comprender que existen importantes diferencias entre los términos "privacidad" e "intimidad", si bien, ambas acepciones son partes de un todo, esto es, el Derecho Fundamental a la intimidad. Así, existe jurisprudencia más o menos restrictiva sobre la delimitación del término "intimidad", pues no resulta nada fácil establecer una línea divisoria que dicte dónde termina la privacidad y dónde comienza la intimidad de la persona.

El TC describe la intimidad del individuo como la esfera más reservada de la vida de las personas, es decir, el ámbito que éstas desean ocultar de los demás por pertenecer a su esfera más privada, delimitándola como el "núcleo central de la personalidad" que debe quedar excluido de todo conocimiento ajeno y cuyo disfrute no es absoluto, puesto que ha de ponderarse al derecho de dirección del empleador y, por tanto, al derecho a la libertad de empresa[45]. Así, elementos tales como, la vivienda, las conversaciones privadas, la religión o creencias, la salud, la vida familiar, etc., quedarán protegidos en virtud del derecho constitucional a la intimidad[46].

La privacidad, sin embargo, se caracteriza por abarcar ciertos aspectos de la personalidad que, aunque se desenvuelvan a vista de algunos y por sí solos no sean relevantes, en su conjunto pueden identificar a un individuo (como por ejemplo, las

[44] Véase el artículo 20.bis ET que se encuentra vigente desde el 7 de diciembre de 2018. Asimismo, este precepto se relaciona con la LOPDGDD que desarrolla los derechos comentados en el texto en los artículos 87 – 91.

[45] Véanse las SSTC 151/1997, de 29 de septiembre; y 231/1988, de 2 de diciembre, que delimitan el derecho a la intimidad del individuo. En este mismo sentido, las SSTC 143/1994, de 9 de mayo; y 57/1994, de 28 de febrero, se pronuncian sobre el derecho a la intimidad alegando que "no es absoluto, al igual que ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho".

[46] Véase la sinopsis del artículo 18 CE elaborada por la profesora ELVIRA PERALES y actualizada por la Letrada de las Cortes Generales Ángeles González Escudero. Disponible en: http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2 (última visita: 12/04/2019).

aficiones de una persona)[47]. De este modo, la privacidad resulta menos restrictiva (y, por ende, menos protegida) y de mayor alcance que la intimidad[48].

Hecha esta aclaración, debemos recordar que lo que protege la Carta Magna es la intimidad personal y familiar de la que goza el trabajador en el marco de una organización empresarial. Y es este derecho el que constantemente está siendo desafiado por el empleo de NTIC en el ámbito laboral debido al carácter fiscalizador de estas herramientas[49].

En este sentido, del binomio derecho a la intimidad y poder de control empresarial surge una problemática que se concreta en dos situaciones: por un lado, el uso personal que los trabajadores pueden hacer de las herramientas informáticas puestas a disposición por el empresario y cuyas consecuencias pueden generar conflictos; y por otro, la necesidad de establecer límites a la vigilancia empresarial que se lleva a cabo a través de dispositivos tecnológicos[50].

En definitiva, la intimidad no es un derecho absoluto, por lo que puede verse limitada debido a la tutela de otros derechos u otros bienes jurídicamente protegidos[51]. Asimismo, cabe la restricción del derecho a la intimidad en caso de que el titular lo autorice a tal efecto y si los tribunales así lo estiman, como veremos.

---

[47] SALGADO SEGUÍN, V., "Intimidad, privacidad y honor en internet", *TELOS 85: Los derechos fundamentales en internet*, TELOS: Cuadernos de Comunicación e Innovación, Madrid, 2010. Disponible en: https://telos.fundaciontelefonica.com/archivo/numero085/intimidad-privacidad-y-honor-en-internet/ (última visita: 12/04/2019).

[48] APARICIO ALDANA, R. K., *Derecho a la intimidad y a la propia imagen en las relaciones jurídico laborales*, Thomson Reuters-Aranzadi, Cizur Menor, 2016, págs. 45 y 46. Véanse las SSTSJ Comunidad Valenciana 567/2012, de 24 de febrero; y Canarias 97/2011, de 3 de marzo, que no estiman que exista una vulneración de la intimidad de los trabajadores que han sido grabados y fotografiados mientras realizaban labores cotidianas del día a día en vía pública y establecimientos de acceso público.

[49] Véase la STS de 26 de septiembre de 2007 (núm. rec. 966/2006), donde DESDENTADO BONETE se menciona la capacidad intrusiva y fiscalizadora que poseen las NTIC. Sobre este extremo también se pronuncia GUDE FERNÁNDEZ cuando dice "…estos sorprendentes niveles de inspección empresarial, alcanzados con los nuevos dispositivos tecnológicos, plantean, sin embargo, importantes problemas ético jurídicos", en su artículo "La videovigilancia laboral y el derecho a la protección de datos de carácter personal", *Revista de Derecho Político*, 2014, núm. 91, pág. 46.

[50] En cuanto al uso particular de instrumentos de trabajo, DESDENTADO BONETE expone que existen dos corrientes a seguir: una tendencia más estricta que estima la autorización expresa del empleador como obligatoria para este uso privado; y una vía más flexible que alude a la existencia "de un hábito social generalizado de dicha herramienta informática para fines particulares por parte de los trabajadores que debe ser tolerado por los empresarios, aún sin autorización expresa (…) de acuerdo con las reglas de la buena fe". Estas dos tendencias son tratadas de manera más amplia y detallada en su ponencia "Nuevas tecnologías y las relaciones laborales" presentada en el *XIII Foro Aranzadi Social 2012-2013*, en Madrid, el 10 de abril de 2013. Véase también SAN MARTÍN MAZZUCCONI, C.; SEMPERE NAVARRO, A. V., *Las TICs en el ámbito laboral*, Francis Lefebvre, Madrid, 2015, págs. 11 y 12.

[51] La sinopsis del artículo 18 CE pone como ejemplo la investigación de la paternidad como límite a la intimidad del progenitor en atención a proteger los derechos de los hijos según el artículo 39 CE. Véase la sinopsis del artículo 18 CE elaborada por la profesora ELVIRA PERALES y actualizada por la Letrada de las Cortes Generales Ángeles González Escudero. Disponible en: http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2 (última visita: 12/04/2019).

2.1.2.- El Derecho Fundamental al secreto de las comunicaciones

El uso de dispositivos electrónicos (véase el teléfono móvil, una tableta, o el ordenador) como herramientas de trabajo puede generar importantes controversias debido al difícil equilibrio entre la facultad de control que posee el empresario y el derecho a la intimidad de sus empleados. Por ello, el derecho al secreto en las comunicaciones también juega aquí un papel importante, pues gracias a este, los trabajadores gozan de confidencialidad en sus conversaciones se encuentren o no dentro de su jornada laboral[52].

Podemos definir la comunicación como el proceso a través del cual se transmiten mensajes entre varias personas, ya sea en forma escrita, mediante sonidos o a través de signos o señales[53].

Así, en virtud del artículo 18.3 CE se "garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial". Al igual que ocurre con el Derecho Fundamental a la intimidad, el artículo 8 CEDH también regula el secreto de las comunicaciones. El objetivo de estos preceptos es evitar la injerencia de terceros (ajenos a una conversación) en la transmisión de mensajes entre un emisor y un receptor. Según ha interpretado el Tribunal Europeo de Derechos Humanos (en adelante, TEDH) se trata de tutelar el secreto de la comunicación en su totalidad, es decir, incluyendo los elementos de que la componen (emisor, receptor, código, medio y contenido)[54].

Puede resultar curiosa la precisión que la CE realiza al referirse a las comunicaciones por vía postal, telegráfica o telefónica. Sin embargo, téngase en cuenta que en el momento de redacción de la CE en 1978 no existían los medios de comunicación electrónicos tal y como hoy los conocemos. Ahora bien, nuestra Carta Magna se configura como un marco teórico general, por lo que debe entenderse que las nuevas formas de comunicación también quedan amparadas bajo la protección de este Derecho Fundamental[55].

En la transmisión de una misma comunicación pueden entrar en juego varios DDFF, si bien, estos se articularán de manera diferente. Ciertamente, esto es lo que ocurre con el

[52] Así lo afirman las SSTC 123/2002, de 20 de mayo, y 114/1984, de 29 de noviembre, entre otras.
[53] Véase la STC 281/2006, de 9 de octubre, FJ 3º.
[54] Véase la STEDH 1984\1, de 2 de agosto, en el asunto Malone contra el Reino Unido, y la STC 114/1984, de 29 de noviembre.
[55] FERNÁNDEZ ESTEBAN, M. L., "Estudio de la jurisprudencia constitucional y ordinaria sobre el secreto de las telecomunicaciones entre particulares, en especial en el ámbito de la empresa", *Revista Aranzadi Doctrinal Civil-Mercantil*, núm. 3, 2000, pág. 38.

derecho a la intimidad y al secreto de las comunicaciones. Así, mientras que el derecho al secreto comprende toda la información contenida en el mensaje transmitido sin tener en cuenta el asunto tratado[56], la vulneración del derecho a la intimidad queda subordinada al contenido del mensaje, pues esta intimidad se verá quebrantada si el tema de la conversación hace referencia a la esfera privada de los comunicantes[57]. Esto significa que, cuando es uno de los interlocutores quien revela la comunicación (ya sea en todo o en parte) no existe lesión del secreto. Sin embargo, el mensaje puede resultar una transgresión del derecho a la intimidad si su contenido así lo hace pues, "entre los interlocutores solo opera la tutela de la intimidad, pero en este caso su eficacia se condiciona a que el contenido de la comunicación sea íntimo", manifestándose así un deber de reserva entre los participantes[58]. En este mismo sentido, las grabaciones realizadas por uno de los participantes de una conversación, sea cual sea el medio o herramienta en que se registre, no conculcan la garantía del artículo 18.3 CE, puesto que esta protección solo interviene frente a personas ajenas al proceso de diálogo[59].

Asimismo, el derecho al secreto de las comunicaciones -al igual que la intimidad- puede verse limitado si el titular da su consentimiento para que este derecho sea restringido.

Llegados a este punto, la cuestión radica en determinar en qué medida un empresario puede tener acceso a las conversaciones que sus empleados realizan a través de las NTIC en el trabajo. Pues bien, la jurisprudencia acepta la existencia de una "autorización tácita" entre los miembros de la relación contractual que aprueba el eventual uso personal de los dispositivos tecnológicos. Esta autorización solo podrá verse contravenida a través de una prohibición expresa y establecida, ya sea por la normativa o

[56] Según, RODRÍGUEZ LAINZ, J. L., "la protección que brinda el art. 18.3 de la CE a cualesquiera comunicaciones es absolutamente independiente de la naturaleza o trascendencia real de la información que se transmite a través de las redes de comunicaciones", en "Análisis del espectro electromagnético de señales Inalámbricas: rastreo de dispositivos wi-fi", *Diario La Ley*, núm. 8588, 2015. Véase también DESDENTADO BONETE, A.; MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012, págs. 189.

[57] Véase la STC 114/1984, de 29 de noviembre, FJ 7º.

[58] LÓPEZ ORTEGA, J. J., "La utilización de medios técnicos de observación" en *La protección jurídica de la intimidad*, IUSTEL, Valencia, 2010, pág. 267.

[59] Véase en este sentido la STC 114/1984, de 29 noviembre. Véase también la STS 678/2014, de 20 de noviembre, sobre una trabajadora que graba una conversación entre ella y su superior sin su consentimiento mientras le hace entrega de la carta de despido en una vía pública. En este caso, el TS resuelve que la grabación de audio no transgrede la protección al secreto de las comunicaciones debido a que este solo protege ante la intromisión de terceros ajenos al mensaje, ni vulnera el Derecho Fundamental a la intimidad personal del empleador, puesto que el contenido de la conversación trata, exclusivamente, sobre temas laborales.

convenio colectivo aplicable, o bien, mediante una orden empresarial[60]. No obstante, las medidas de control empresarial deben ser valoradas en atención al uso que los empleados les dan y a las órdenes que el empresario haya dispuesto[61], pues no existen reglas universales y habrá que atender a las circunstancias particulares en cada caso[62].

2.1.3.- El Derecho Fundamental a la protección de datos

El derecho a la protección de datos de carácter personal se configura como "un derecho autónomo e independiente que consiste en un poder de disposición y control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero", cuya finalidad es garantizar el control del individuo sobre sus propios datos, en cuanto a su uso y destino, con el objetivo de evitar "su tráfico ilícito o lesivo para la dignidad y derecho de los afectados", según establece el TC[63].

Este derecho, también conocido como *habeas data* o autodeterminación informativa, ha sido denominado como un "Derecho Fundamental no escrito"[64], puesto que la CE no lo regula de manera explícita[65].

El artículo 18.4 CE señala que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", por lo que han sido los tribunales los que han venido interpretando que este precepto se configura como un Derecho Fundamental con sentido propio; esto es, el Derecho Fundamental a la protección de datos[66].

---

[60] Véase la STC 170/2013, de 7 de octubre, en la que el convenio colectivo aplicable contenía un precepto sobre el uso exclusivamente profesional del correo electrónico propiedad de la empresa, constituyendo como infracción grave el uso para diferentes fines.
[61] Así lo afirma el TC en su sentencia 241/2012, de 17 de diciembre.
[62] ROQUETA BUJ, R., "El derecho a la intimidad de los trabajadores", *Protección jurídica de la intimidad*, IUSTEL, Madrid, 2012, págs. 444 – 446.
[63] Véase la STC 292/2000, de 30 de noviembre, FJ 2º.
[64] Véase VILLAVERDE MENÉNDEZ, I., "La Jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos" en *La protección de datos de carácter personal en los centros de trabajo* (Dir. FARRIOLS I SOLÀ, A.), Ediciones Cinca, Madrid, 2006, pág. 52.
[65] GOÑI SEIN, J. L., "Los derechos fundamentales inespecíficos en…", *Op. Cit*., pág. 40.
[66] La STC 94/1998, de 4 de mayo, declaró que el artículo 18.4 CE reconoce el derecho a la protección de datos de carácter personal. En este sentido, véanse también las SSTC 292/2000; y 290/2000, de 30 de noviembre.

Asimismo, la protección de los datos personales cuenta con su propia normativa de desarrollo, esto es, la LOPDGDD y el Reglamento General de Protección de Datos (en adelante, RGPD)[67].

Resulta destacable la importancia que el tratamiento de datos tiene en las RRLL[68]. En este sentido, a lo largo de la vida de una organización se recogen gran cantidad de datos personales de los trabajadores (algunos necesarios para la propia relación contractual como son: el nombre del empleado, su DNI, o su número de la Seguridad Social) cuyo procesamiento se ha visto facilitado sobremanera por la incursión de las NTIC en el mundo empresarial[69].

Para comprender mejor que es un dato de carácter personal, es necesario acudir al RGPD, en cuyo articulado se identifica como dato personal "cualquier información concerniente a personas físicas identificadas o identificables", así como "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables" [70]. Por tanto, la normativa sobre protección de datos debe aplicarse en tanto en cuanto una persona pueda ser reconocida, de manera directa o indirecta, a través de los datos habidos sobre ella.

Un claro ejemplo sobre la gran incidencia que posee este derecho en el ámbito de las RRLL podemos verlo en el uso de cámaras de videovigilancia por parte del empresario. Esta herramienta de control ha favorecido el desarrollo de la normativa en este sentido, pues la imagen de un trabajador comporta un dato de carácter personal en la medida en que este identifica o hace identificable a una persona[71]. Así, la reciente LOPDGDD ha introducido varios preceptos sobre videovigilancia que recogen las recientes líneas jurisprudenciales, esto es, entre otras, el deber de información sobre la

[67] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

[68] El artículo 4.2 RGPD define el tratamiento de datos como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

[69] LLAMOSAS TRAPAGA, A., *Relaciones laborales y nuevas… Op. Cit.*, págs. 100 y 101.

[70] El artículo 5.f) RGPD determina que una persona identificable es aquella "cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados."

[71] ARRABAL PLATERO, P., "La videovigilancia laboral…", *Op. Cit*., pág. 5.

ubicación y finalidad de las cámaras, o la prohibición de grabación en lugares de descanso, como veremos[72].

El derecho a la protección de datos, al igual que los derechos a la intimidad y al secreto de las comunicaciones, no es absoluto, y se encuentra limitado por la exigencia informativa que establece el RGPD. Este requerimiento supone al responsable del tratamiento la obligación de poner en conocimiento del interesado (el sujeto titular del derecho) el registro al que sus datos son sometidos y la finalidad que tiene este almacenamiento.

El deber informativo resulta imprescindible para los llamados "derechos ARCO", que se configuran como un grupo de derechos de los que disponen los ciudadanos sobre sus datos personales. Los responsables del tratamiento deben facilitar el pleno ejercicio de estos derechos a través del cumplimiento de su deber informativo[73]. Los derechos ARCO tradicionalmente han hecho referencia a los derechos de acceso, de rectificación, de cancelación y de oposición; si bien, el reciente RGPD ha incorporado dos más, como son el derecho de supresión y el derecho a la portabilidad de los datos personales[74].

En cuanto al consentimiento que pueda dar el afectado, este no será un límite en el ámbito de las RRLL, pues en caso de mediar un contrato de índole laboral la autorización se considerará concedida de manera tácita[75]. Sin embargo, el consentimiento expreso se hace necesario en caso de que el empresario pueda tener acceso a cierto tipo de datos de carácter especial, como los referidos a la salud de los trabajadores[76].

Los datos de salud resultan de gran relevancia, puesto que la normativa en materia de prevención de riesgos laborales exige al empresario el deber de vigilar la salud de los trabajadores[77]. Así, los empleadores pueden realizar exámenes médicos de sus empleados con el pertinente consentimiento. No obstante, esta autorización no será necesaria si el

[72] Artículos 22 y 89 LOPDGDD.
[73] BLÁZQUEZ AGUDO, E. M., *Aplicación práctica de la protección de datos en las relaciones laborales,* Wolters Kluwer, Madrid, 2018, pág. 105.
[74] Artículos 15 – 21 RGPD.
[75] El artículo 9.11 RGPD define el consentimiento del afectado por el tratamiento de sus datos personales como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".
[76] Según el artículo 9 RGPD son datos de carácter especial los datos personales que "revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física".
[77] Véanse los artículos 14.2, 22 y 28.3 de la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales.

control de salud resulta indispensable en atención a los parámetros que establece la Ley de Prevención de Riesgos Laborales para determinados puestos de trabajo[78].

Asimismo, debido a que este tipo de datos son considerados como sensibles para el trabajador, los resultados del informe médico solo podrán ser puestos en conocimiento del propio trabajador. El empresario, no obstante, solo tendrá derecho a conocer si el trabajador es "apto" o "no apto" para el puesto en cuestión[79].

Como hemos visto, los DDFF a la intimidad, al secreto de las comunicaciones y a la protección de datos, actúan como límite al control del empresario. El carácter preferente que la CE otorga a los DDFF hace necesario modular el alcance de la facultad de vigilancia empresarial con el fin de no lesionar el núcleo esencial de estos derechos.

En definitiva, la cuestión radica en determinar en qué medida un empresario puede controlar la actividad que sus empleados realizan, ya sea a través de la vigilancia de los medios tecnológicos (véase la videovigilancia o la geolocalización); ya sea por medio de las herramientas informáticas puestas a disposición por la empresa (como por ejemplo, el ordenador).

2.2.- La prueba prohibida en el proceso laboral

El control empresarial a través de las NTIC puede resultar una herramienta muy útil en la medida en que los dispositivos digitales permiten dejar constancia de posibles infracciones laborales, convirtiéndose así en un medio de prueba capaz de acreditar una sanción o, incluso, el despido de un trabajador[80]. Sin embargo, la vigilancia a través de las nuevas tecnologías puede resultar un método potencialmente invasivo en relación con los DDFF de los trabajadores[81]. Por ello, la licitud de las medidas empresariales de control es tan importante en el ámbito laboral, pues si estas vulneran los derechos de los trabajadores, las pruebas obtenidas como consecuencia de su práctica no serán válidas en el proceso[82].

---

[78] BLÁZQUEZ AGUDO, E. M., *Aplicación práctica de la…Op. Cit.*, págs. 140 y 141.

[79] En este sentido, véase el informe jurídico núm. 0240/2009 de la AEPD. Disponible en: https://www.aepd.es/informes/historicos/2009-0240.pdf (última visita: 10/06/2019).

[80] RODRÍGUEZ ESCANCIANO, S., RODRÍGUEZ ESCANCIANO, S., *Poder de Control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, Valencia, 2015, págs. 9 y 10.

[81] Así lo afirma FUENTES SORIANO, cuando dice que "si bien es cierto que las modernas tecnologías facilitan enormemente la vida de los ciudadanos, resulta igualmente cierto que su uso generalizado constituye una permanente amenaza para derechos fundamentales", en "Videos, comunicación electrónica y redes sociales: cuestiones probatorias", *Práctica de Tribunales*, núm. 135, Wolters Kluwer, 2018, pág. 3.

[82] Señala GARCÍA-PERROTE ESCARTÍN que "ni los poderes empresariales de dirección y control sobre la actividad del trabajador, ni tampoco los intereses públicos ligados a la fase probatoria del proceso

La prueba puede ser definida como la actividad procesal encaminada a acreditar los hechos en los que se fundamenta la pretensión de la parte que la propone, con el propósito de obtener la convicción del órgano judicial sobre la veracidad de los hechos[83].

Todos los ciudadanos tienen derecho a "utilizar los medios de prueba pertinentes para su defensa" con el fin de demostrar los hechos que se invocan como ciertos, tal y como reza el artículo 24 CE. Los medios de prueba son los canales que pueden hacer valer las partes de un proceso para presentar los elementos probatorios ante el juez[84]. Así, tal y como establece el artículo 299 de la Ley de Enjuiciamiento Civil (en adelante, LEC)[85], los medios de prueba de que se podrá hacer uso en un juicio son: el interrogatorio de las partes, los documentos públicos y privados, el dictamen de peritos, el reconocimiento judicial, y el interrogatorio de testigos. Seguidamente, se establece otro medio de prueba en clara referencia a las evidencias de naturaleza tecnológica, esto es, "los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso".

En el ámbito laboral, el artículo 90.1 de la Ley Reguladora de La Jurisdicción Social (en adelante, LRJS)[86] establece que las partes "podrán servirse de cuantos medios de prueba se encuentren regulados en la Ley para acreditar los hechos controvertidos o necesitados de prueba, incluidos los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de datos, que deberán ser aportados por medio de soporte adecuado y poniendo a disposición del órgano jurisdiccional los medios necesarios para su reproducción y posterior constancia en autos"[87]. Así, la ley reconoce un listado no exhaustivo sobre los medios de prueba que las partes pueden aportar en sede judicial[88].

---

encaminados a la averiguación de la verdad, pueden prevalecer sobre aquellos derechos fundamentales", en "Prueba y Proceso Laboral", *Derecho Privado y Constitución*, núm. 4, 1994, pág. 169.

[83] Definición elaborada a partir de la descripción del término "prueba" que realiza el Diccionario del español jurídico de la Real Academia Española. Disponible en: https://dej.rae.es/lema/prueba (última visita: 25/04/2019). En este sentido, véase también GIMENO SENDRA, V., *Introducción al Derecho Procesal*, Ediciones Jurídicas Castillo de Luna, Madrid, 2017, pág. 371; y GARBERÍ LLOBREGAT, J., *El nuevo proceso laboral*, Civitas, Madrid, 2011, pág. 286.

[84] En este sentido, véase el seminario "El proceso y la prueba" cuyas ponentes son LÓPEZ YAGÜES, FUENTES SORIANO y FERNÁNDEZ LÓPEZ, celebrado en la Universidad Miguel Hernández de Elche el 24 de mayo de 2018. Disponible en: https://www.youtube.com/watch?v=ifZQPrRIzck&t=3068s (Ultima visita: 01/05/2019).

[85] Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

[86] Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social.

[87] Véanse también los artículos 382 y 384 LEC.

[88] En este sentido, véanse las SSTSJ Canarias 19/2016, de 22 de enero; Cantabria 843/2015, de 10 de noviembre; y Cataluña 3980/2015, de 17 de junio.

La prueba tecnológica hace referencia a aquella información que, o bien se obtiene como resultado de emplear una técnica informática (un correo electrónico o la imagen de un trabajador que se encuentra bajo videovigilancia)[89], o bien queda registrada en un soporte de carácter informático (el disco duro de un ordenador, un *pen drive*, o un CD)[90].

El empleo de pruebas tecnológicas en el marco de la Jurisdicción Social ha aumentado de manera paralela al uso de las NTIC en las RRLL[91]. Las pruebas de naturaleza electrónica permiten el almacenamiento de gran cantidad de datos, si bien su tratamiento deberá ser el de prueba documental, pues resultan una evolución de estas, donde el elemento diferenciador, sin duda, es el soporte sobre el que se almacena la información[92].

Ahora bien, este tipo de elementos de convicción posee una gran desventaja con respecto de los medios más tradicionales, esto es, pueden resultar fácilmente alterables. Para tratar de salvar esta cuestión, los tribunales, además de utilizar las actas notariales con el objeto de certificar la autenticidad de los contenidos expuestos, han recurrido a técnicas más avanzadas tales como la encriptación de la información[93].

Las pruebas -como norma general-, son practicadas durante el juicio oral y, posteriormente, el órgano judicial estima si estas acreditan o no los hechos aducidos por las partes[94]. Pero para que se dé dicha práctica, las pruebas han de ser lícitas[95]. En caso contrario, ni las pruebas, ni los efectos que pudieran derivarse de ellas podrán tenerse en cuenta durante un proceso judicial quedando, por tanto, prohibidas[96].

En cuanto a los términos "prueba prohibida" y "prueba ilícita", cabe decir, que la doctrina viene utilizando ambos conceptos de manera análoga para referirse a los elementos probatorios obtenidos con vulneración de los DDFF, independientemente de

---

[89] Véanse los artículos 382 y 383 LEC.

[90] Véase el artículo 384 LEC. En este sentido, véase también BLÁZQUEZ AGUDO, E. M., *Aplicación práctica de la… Op. Cit.*, pág. 211.

[91] Véase la entrada "La prueba digital en el ámbito laboral ¿son válidos los pantallazos?" del abogado Raúl Rojas Rosco en su blog http://raulrojas.es. Disponible en: http://raulrojas.es/234-2/ (última visita: 30/04/2019).

[92] Véase GARCÍA-PERROTE ESCARTÍN, I., "La prueba en el proceso de trabajo", *Relaciones Laborales*, núm. 12, 2001; y BLÁZQUEZ AGUDO, E. M., *Aplicación práctica de la…Op. Cit.*, pág. 211.

[93] SAN MARTÍN MAZZUCCONI, C.; SEMPERE NAVARRO, A. V., *Las TICs en el… Op., Cit.,* pág. 33. Véase en este sentido, la STS 300/2015, de 19 de mayo y la STSJ Cataluña 1197/2012, de 14 de febrero.

[94] En este sentido, véase GARBERÍ LLOBREGAT, J., *El nuevo proceso laboral… Op. Cit.,* pág. 291. Véanse también los artículos 87.1 y 87.2 LRJS, 289.1 y 289.2 LEC.

[95] Según el artículo 90.2 LRJS, "no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas".

[96] Dice GARCÍA-PERROTE ESCARTÍN que esto es así porque "aunque dichas pruebas demuestren lo que se quería probar, ningún partido se podrá sacar de ellas en el seno del proceso, en el que habrá que tenerlas por inexistentes, en "Prueba y Proceso Laboral"… *Op. Cit.*, pág. 191. Véase el artículo 287 LEC.

la jurisdicción que conozca del pleito en cuestión. No obstante, téngase en cuenta que existen otras expresiones como "prueba irregular" y "prueba ilegal" que, si bien suelen emplearse como sinónimos de "prueba ilícita" y "prueba prohibida", poseen un significado distinto[97]. Así, la prueba irregular o ilegal es aquella en cuya obtención se vulnera la legalidad ordinaria y/o no se respeta la normativa procesal[98].

La doctrina de la prueba ilícita encuentra su fundamento en la primacía de la que gozan los DDFF en nuestro ordenamiento jurídico, cuya posición de superioridad obedece a su consideración de elementos esenciales del Derecho y a su conexión con la dignidad de la persona[99].

La tesis de la prueba prohibida, también conocida como la "regla de la exclusión probatoria", fue introducida por primera vez en nuestro país por la importante STC 114/1984, de 29 de noviembre, que analizaba la validez de la grabación de audio de un trabajador[100].

Los hechos que traen causa esta sentencia nacen del despido disciplinario de un trabajador "por infracción de las obligaciones de lealtad y buena fe en sus relaciones para con la empresa"[101]. El trabajador, un redactor del periódico Información, realizó ciertos comentarios en contra de la editorial mientras hablaba a través del teléfono con un tercero, quien grabó la conversación y se la hizo llegar a la empresa.

En este contexto, el intérprete constitucional declaró que el Derecho Fundamental al secreto de las comunicaciones no fue vulnerado, pues este no se activa entre los interlocutores que forman parte de una misma conversación, estimando así la prueba

---

[97] Sobre la diferenciación de estos conceptos véase MIRANDA ESTRAMPES, M., "La prueba ilícita: la regla de exclusión probatoria y sus excepciones", *Revista Catalana de Seguretat Pública*, núm. mayo 2010, pág. 131 y 132; GIMENO SENDRA, V., *Introducción al Derecho Procesal… Op. Cit.,* pág. 348; y DESDENTADO BONETE, A.; MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y… Op. Cit.,* págs. 125 – 127.

[98] ARMENTA DEU, M. T., *La prueba ilícita (un estudio comparado),* Marcial Pons, Madrid, 2011, pág. 95. En este sentido, véase la STS de 2 de diciembre de 2014 (núm. rec. 97/2013), que declara nula la prueba que no se aportó con la debida antelación.

[99] En este sentido se manifiesta ARRABAL PLATERO cuando afirma que "…los jueces son constantes en mantener la defensa de los derechos fundamentales haciéndolos prevalecer, aunque no de forma absoluta, frente a la potestad de control del empleador", en "La videovigilancia laboral…", *Op. Cit*., pág. 4. Véanse las SSTC 308/2000, de 18 de diciembre; 98/2000, de 10 de abril; 143/1994, de 9 de mayo; y 57/1994, de 28 de febrero.

[100] La teoría de la prueba prohibida tiene su origen en el Derecho norteamericano, concretamente, en el caso *U.S. v. Janis (1976)* de la Corte Suprema de los Estados Unidos que excluye del proceso las pruebas obtenidas lesionando la IV Enmienda (El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas).

[101] STC 114/1984, de 29 de noviembre, antecedente de hecho 1º.

tecnológica como lícita. Consiguientemente, el TC confirmó la procedencia del despido del trabajador.

Sobre las pruebas conseguidas con menoscabo de DDFF, la STC 114/1984 fija que estas no son admisibles en el proceso, por lo que no pueden desplegar sus efectos. Esta doctrina asevera que la admisibilidad de pruebas ilícitamente obtenidas entra en clara colisión con el artículo 24.2 CE sobre la presunción de inocencia y las garantías procesales, así como con el artículo 14 CE sobre el principio de igualdad entre las partes[102].

No obstante, el Tribunal pone de manifiesto que "no existe en nuestro ordenamiento jurídico una norma expresa que imponga la no consideración como prueba de aquellas propuestas por las partes y obtenidas antijurídicamente"[103]. Esta afirmación, provocó que la posterior Ley Orgánica del Poder Judicial (en adelante, LOPJ)[104] regulase la doctrina de la prueba ilícita en su artículo 11.1 reconociendo que "no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales"[105].

Como puede observarse, la LOPJ distingue entre dos tipos de pruebas ilícitas: por un lado, las directas u originarias, esto es, las obtenidas violentando DDFF; y, por otro lado, las pruebas indirectas o derivadas, que son las que resultan como consecuencia de otras que son ilícitas[106].

Esta diferenciación introdujo en nuestro sistema legal el llamado "efecto reflejo de la prueba prohibida" o "doctrina de los frutos de árbol envenenado", cuyo fin es asegurar el derecho a un proceso con todas las garantías[107]. El efecto reflejo se basa en la relación de dependencia existente entre los elementos probatorios que nacen con ocasión de otros prohibidos en el proceso. Este vínculo provoca que una prueba prohibida irradie su ilicitud a las que se deriven de ella[108]. En otras palabras, las pruebas que, aun siendo

[102] STC 114/1984, de 29 de noviembre, FJ 7º.
[103] Son numerosas las sentencias que han venido aplicando la regla de la exclusión probatoria, a modo de ejemplo véanse las SSTC 28/2002, de 11 de febrero; 50/2000, de 28 de febrero; 49/1999, de 5 de abril; 81/1998, de 2 de abril; 49/1996, de 26 de marzo; 181/1995, de 11 de diciembre; 85/1994, de 14 de marzo; 80/1991, de 15 de abril; 64/1986, de 21 de mayo; 107/1985, de 7 de octubre.
[104] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.
[105] La misión del artículo 11.1 LOPJ es "garantizar la indemnidad de los derechos fundamentales", según FUENTES SORIANO en "Videos, comunicación electrónica y…", *Op. Cit.*, pág. 6.
[106] ATS de 18 de junio de 1992 (núm. rec. 610/1990).
[107] MIRANDA ESTRAMPES, M., "La prueba ilícita: la regla…", *Op. Cit.*, pág. 136.
[108] Según ARMENTA DEU, la teoría de la eficacia refleja supone que "la ilicitud de la prueba arrastra a todas las restantes aunque hubieran sido obtenidas o practicadas de forma lícita siempre que tengan origen en la primera", en *La prueba ilícita… Op. Cit.,* pág. 121. En este sentido, véanse las SSTC 66/2009, de 9 de marzo; 261/2005, de 24 de octubre; 28/2002, de 11 de febrero; 136/2000, de 10 de julio; 49/1999, de 5 de

obtenidas de forma legítima procedan de otras que conculquen DDFF, serán igualmente eliminadas del proceso[109].

Así las cosas, el carácter garantista de la teoría de la prueba prohibida ha venido permitiendo la absolución de investigados cuando la acusación se fundamenta en pruebas obtenidas, directa o indirectamente, lesionando los DDFF. Este efecto tan perjudicial ha llevado al TC a admitir ciertas limitaciones en la regla de la exclusión probatoria y en los efectos reflejos de la nulidad[110].

En este sentido, la jurisprudencia busca tutelar los DDFF de los ciudadanos, entendiendo que la consecuencia procesal de una prueba que lesione los DDFF no siempre debe ser su prohibición. Este punto de vista menos restrictivo, tolera el empleo de pruebas obtenidas con lesión de DDFF ante determinadas situaciones tales como: la actuación policial de buena fe (los elementos probatorios que pueda obtener la policía como consecuencia de su actividad investigadora serán lícitos siempre que su actuación sea de buena fe)[111]; la excepción de la fuente independiente (no existe conexión causal entre la prueba originaria y la derivada)[112]; un descubrimiento inevitable (la prueba lesiva de DDFF resultará válida en el proceso si esta hubiese podido ser conocida a través de otras vías que sí los respeten)[113]; un hallazgo casual (es lícito lo encontrado de manera casual aunque la prueba de la que derive sea ilícita)[114]; y el nexo causal atenuado (la conexión entre la prueba ilícita directa y la indirecta es tan débil, que aunque existe, no se toma en cuenta y se permite el uso en el proceso de la prueba prohibida derivada)[115].

---

abril; 81/1998, de 2 de abril; 86/1995, de 6 de junio; 107/1985, de 7 de octubre; y 114/1984, de 29 de noviembre.

[109] En este sentido, la STS 636/2008, de 2 de octubre, expresa que "no es necesario que la prueba derivada sea obtenida de manera ilegítima, sino que basta con que proceda de una que se ha conseguido de manera no amparada por el marco legal vigente".

[110] En este sentido, la STC 49/1999, de 5 de abril, manifiesta en su FJ 12º que, "en definitiva, es la necesidad de tutelas los derechos fundamentales la que, en ocasiones, obliga a negar eficacia probatoria a determinados resultados cuando los medios empleados para obtenerlos resultan constitucionalmente ilegítimos".

[111] MIRANDA ESTRAMPES, M., "La prueba ilícita: la regla…", *Op. Cit.*, pág. 140. Véase también la STC 22/2003, de 10 de febrero, que acepta la prueba obtenida por la actuación de la Policía que realiza un registro de la vivienda de un detenido sin la autorización del titular, vulnerando así el Derecho Fundamental a la inviolabilidad del domicilio.

[112] Según MIRANDA ESTRAMPES, esta tendencia no es en realidad una excepción, "sino que su reconocimiento es consecuencia de la propia delimitación del alcance de la regla de exclusión", en "La prueba ilícita: la regla…", *Op. Cit.*, pág. 143. Véase también ARMENTA DEU, M. T., *La prueba ilícita… Op. Cit.*, págs. 121 y 122.

[113] MIRANDA ESTRAMPES, M., "La prueba ilícita: la regla…", *Op. Cit.*, pág. 144. Véase también ARMENTA DEU, M. T., *La prueba ilícita… Op. Cit.,* pág. 122.

[114] ARMENTA DEU, M. T., *La prueba ilícita… Op. Cit.,* pág. 122.

[115] La excepción del nexo causal atenuado es en realidad una variante de la llamada "fuente independiente" tal y como afirma MIRANDA ESTRAMPES en "La prueba ilícita: la regla…", *Op. Cit.*, pág. 146. ARMENTA DEU llama a esta excepción "irregularidad saneada", en *La prueba ilícita… Op. Cit.,* pág. 123.Vease la STC

Del mismo modo, la doctrina de la conexión de antijuricidad también puede operar como límite a la eficacia refleja de las pruebas pues, "si la prueba refleja resulta jurídicamente ajena a la vulneración del derecho y la prohibición de valorarla no viene exigida por las necesidades esenciales de tutela del mismo cabrá entender que su efectiva apreciación es constitucionalmente legítima", tal y como establece el TC[116].

Como se ha visto a lo largo del texto, los derechos que la CE califica como fundamentales juegan un papel clave en la validez de las pruebas en todos los órdenes jurisdiccionales. El sistema legal español confiere a los DDFF una posición preeminente respecto del resto de derechos convirtiéndolos en un elemento vertebrador de toda la sociedad. Así, su respeto o lesión en la obtención de elementos probatorios determinarán, en muchos casos, la ilicitud de las pruebas. No obstante, los DDFF no son absolutos, existiendo determinados supuestos en los que cabe su legítima restricción, siempre que se cumplan ciertos requisitos.

En lo que se refiere al ámbito laboral, la jurisprudencia ha venido exigiendo dos criterios que debe cumplir toda medida de control empresarial para que las pruebas que se deriven de la misma sean válidas y admisibles en un proceso[117].

En primer lugar, las medidas de control empresarial deben estar debidamente justificadas, es decir, la motivación debe ser objetiva sin que exista un "medio razonable para lograr una adecuación entre el interés del trabajador y el de la organización en que se integra"[118].

A esto se suma un segundo criterio donde las medidas de vigilancia deberán someterse al llamado "test de proporcionalidad". Este criterio constitucional, que viene siendo aplicado en el orden social desde la STC 99/1994, de 11 de abril, busca equilibrar los bienes en conflicto ponderando los intereses de ambas partes aplicando un triple juicio: el de idoneidad, el de necesidad y el de proporcionalidad en sentido estricto.

86/1995, de 6 de junio, donde el magistrado hace referencia a esta excepción con lo que llama "prueba jurídicamente independiente".

[116] La doctrina de la conexión de antijuricidad se inició en España con la STC 81/1998, de 2 de abril, que establece que "las pruebas reflejas son desde un punto de vista intrínseco, constitucionalmente legítimas" (FJ 4º).

[117] Véase en este sentido la ponencia de CAVAS MARTÍNEZ, "Los Derechos y Libertades Fundamentales en materia laboral", realizada en el marco del I Seminario del Área de Derecho del Trabajo y la Seguridad Social y que tuvo lugar el 23 de febrero de 2015 en la Universidad Miguel Hernández de Elche (Alicante). Disponible en: https://www.youtube.com/watch?v=fECK5u0FO6A (última visita: 15/03/2019).

[118] STC 99/1994, de 11 de abril, FJ 7º. En este sentido, la STC 1/1998, de 12 de enero, afirma que "aunque la relación laboral tiene como efecto típico la supeditación de ciertas actividades a los poderes empresariales, no basta con la sola afirmación del interés empresarial para restringir los derechos fundamentales del trabajador".

En este sentido, una medida es idónea cuando "es susceptible de conseguir el objetivo propuesto"; es decir, el juicio de idoneidad es superado si la medida es capaz de cumplir con la finalidad que busca el empresario. Asimismo, la medida será necesaria cuando no exista otro medio menos restrictivo de los DDFF de los trabajadores que cumpla la finalidad buscada con el mismo grado de eficacia; en otras palabras, la medida debe resultar indispensable. Y, finalmente, la medida será equilibrada si de ella se derivan más beneficios que desventajas[119].

Estas tres condiciones son de naturaleza acumulativa, esto es, la no superación de cualquiera de ellas supondrá la ilicitud de la medida empresarial por lesionar los DDFF de los trabajadores. En consecuencia, el elemento probatorio que se haya podido obtener con ocasión de la vigilancia ilegítima será nulo.

Así las cosas, el triple juicio de proporcionalidad resulta insuficiente para valorar la licitud de cualquier tipo de medida empresarial, habiendo de examinar las circunstancias concretas de cada caso[120]. Sirva de ejemplo la STC 29/2013, de 11 de febrero, donde el intérprete constitucional declara la ilicitud de la medida empresarial de videovigilancia a pesar de que superar el test de proporcionalidad. El TC estima que el empresario no cumple con su deber informativo -núcleo esencial del derecho a la protección de datos- sobre el tratamiento que está realizando de los datos personales de sus trabajadores.

En resumen, las medidas empresariales restrictivas de los DDFF a la intimidad y al secreto de las comunicaciones serán legítimas cuando resulten justificadas, idóneas, necesarias y proporcionadas, con las limitaciones ya comentadas en relación con el consentimiento del trabajador. Sin embargo, cuando el control empresarial entre en conflicto con el derecho a la autotutela informativa, será necesario que la medida cumpla con los requisitos que fija la normativa en materia de protección de datos, siendo el más relevante el deber informativo.

En cuanto a los efectos que la prohibición de las pruebas puede tener en un procedimiento judicial, el artículo 11.1 LOPJ establece que los tribunales no podrán admitir ni valorar pruebas ilícitas. Sin embargo, en caso de ser admitida una prueba que

[119] Véanse las SSTC 96/2012, de 7 de mayo; 37/1998, de 17 de febrero, FJ 8º; 207/1996, de 16 de diciembre, FJ 4º; 55/1996, de 28 de marzo, FJ 6º – 9º; y 66/1995, de 8 de mayo, FJ 5º.

[120] GOÑI SEIN se pronuncia en este sentido afirmando que "no puede configurarse la legalidad de la decisión empresarial solo supeditado a que se supere el denominado triple test de proporcionalidad y sin contemplar la eventual proyección de los derechos o expectativas surgidas de las reglas adoptadas por el propio empresario", en "Los derechos fundamentales inespecíficos en…", *Op. Cit*., pág. 67.

lesione DDFF, tanto las partes procesales como el órgano judicial podrán solicitar su impugnación[121].

El artículo 11.1 LOPJ es interpretado de manera desigual tanto por la doctrina como por la jurisprudencia, no obstante, ambos sectores aceptan que el conocimiento de la verdad no debe justificar la admisión de cualquier elemento probatorio. En este sentido, la cuestión más problemática gira en torno a la eficacia refleja de las pruebas ilícitas y sus excepciones. Por ello, será necesario analizar cada caso en profundidad atendiendo a las circunstancias particulares del procedimiento en cuestión.

La superioridad que nuestro ordenamiento jurídico confiere a los DDFF hace necesaria su protección declarando la ineficacia de las pruebas que los vulneren. No obstante, la jurisprudencia permite la limitación de los DDFF en aras de satisfacer otras necesidades constitucionalmente protegidas, como es, el interés empresarial. Así, es posible restringir los DDFF de los trabajadores a través del triple juicio de ponderación, siempre y cuando se preserve el núcleo esencial del derecho.

En definitiva, el *quid* de la cuestión reside en conocer los límites del control empresarial a la luz de las nuevas tecnologías. Así, resulta clave aclarar cuándo el poder de control del empresario lesiona los DDFF de los trabajadores y cuándo la vigilancia resulta legítima. Sobre este extremo no existe normativa específica, por lo que son los tribunales los encargados de dilucidar dicha incógnita, adaptando la doctrina general a los nuevos casos que la generalización de las NTIC trae consigo.

[121] Véanse en este sentido los artículos 90.2 LRJS y 287 LEC.

EPÍGRAFE II.- LAS NUEVAS TECNOLOGÍAS COMO MEDIOS DE CONTROL EMPRESARIAL

La progresiva implantación de las NTIC en el mundo laboral ha originado grandes cambios en las RRLL. Actos como la firma electrónica del contrato de trabajo, el uso sindical de la intranet de la empresa, o el envío del recibo de salarios en formato virtual permiten dar cuenta de cómo las NTIC se han introducido en todos los ámbitos de la vida empresarial[122].

Esta generalización tecnológica también ofrece al empresario nuevas formas de control que le permiten verificar el efectivo cumplimiento contractual de los trabajadores a través de herramientas como: los dispositivos de grabación de audio, las cámaras de videovigilancia, la monitorización del ordenador que el trabajador, la vigilancia sobre las comunicaciones electrónicas, el seguimiento de los dispositivos de geolocalización y el control biométrico de los trabajadores.

Los nuevos mecanismos de control permiten una mayor eficacia y comodidad para el empresario, en relación con la tradicional vigilancia basada en la visualización directa de los trabajadores[123]. Sin embargo, los dispositivos digitales también pueden resultar muy invasivos para el trabajador, pues a través de ellos la empresa tiene la posibilidad de obtener información que va más allá de verificar el mero cumplimiento de la prestación laboral y las obligaciones contractuales[124].

En este sentido, el ejercicio de un control intenso por parte del empresario puede lesionar los DDFF de los trabajadores y entrar en conflicto especialmente con los relativos a la intimidad, al secreto a las comunicaciones y a la protección de datos[125]. Así, la legitimidad del uso de las medidas de control cobra especial relevancia en relación con las decisiones disciplinarias que la empresa pueda adoptar, ya que el resultado de la vigilancia puede ser utilizado como elemento probatorio a fin de acreditar irregularidades cometidas por los trabajadores.

Asimismo, conviene recordar que hasta finales del 2018 la regulación normativa en relación con el uso de medios digitales en el marco de las RRLL era escasa, hecho que ha favorecido la proliferación de conflictos laborales en este sentido. De modo que, debido

[122] SAN MARTÍN MAZZUCCONI, C.; SEMPERE NAVARRO, A. V., *Las TICs en el… Op., Cit.,* pág. 10.
[123] SAN MARTÍN MAZZUCCONI, C.; SEMPERE NAVARRO, A. V., *Las TICs en el… Op., Cit.*, pág. 39.
[124] RODRÍGUEZ ESCANCIANO, S., *Poder de Control Empresarial… Op. Cit.*, págs. 32 y 33.
[125] GUDE FERNÁNDEZ, A., "La videovigilancia laboral y…", *Op. Cit.*, pág. 47.

a la entrada en vigor de la LOPDGDD, nos encontramos ante una fase de adaptación a los nuevos cambios que dicha ley establece.

La LOPDGDD resulta de gran importancia por regular, por primera vez en España, ciertos aspectos en relación con los derechos digitales en el ámbito laboral. Entre sus modificaciones más importantes, destacan las referidas al derecho a la intimidad frente al uso de herramientas tecnológicas (con referencias concretas a las cámaras de video, la grabación de audio y los instrumentos de geolocalización), al tratamiento de datos derivado de la videovigilancia, al derecho a la desconexión digital, y a los derechos digitales en la negociación colectiva[126].

Otra modificación importante es la inclusión del artículo 20.bis ET. Este precepto, denominado "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión", expresa lo siguiente: "Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales". De manera similar, el Estatuto del Empleado Público recoge este derecho en su artículo 14.j.bis[127].

Con todo, debido a que la citada normativa es todavía reciente, han sido los tribunales los encargados de resolver los conflictos surgidos de la confrontación entre las medidas digitales de vigilancia adoptadas por el empresario y los DDFF de los trabajadores[128]. En consecuencia, cabe plantearse cuáles son las condiciones que la actuación empresarial debe cumplir para afirmar que su uso no lesiona ningún derecho constitucionalmente protegido.

En este orden de ideas, el presente trabajo tiene por objeto estudiar el difícil equilibrio entre la facultad de vigilancia del empresario y los derechos de los trabajadores a través de diferentes formas de control laboral como son: los mecanismos audiovisuales,

[126] Véanse los artículos 22, 87 – 91 LOPDGDD.

[127] El artículo 14.j bis) del Estatuto del Empleado Público expresa que "los empleados públicos tienen los siguientes derechos de carácter individual en correspondencia con la naturaleza jurídica de su relación de servicio: (…) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

[128] En este sentido, FUENTES SORIANO afirma que "…el TC ha ido perfilando una interesante doctrina en función de la cual la grabación de la actividad laboral de los trabajadores en el seno de la empresa no tiene por qué afectar, en términos generales, a su derecho a la intimidad…", en "Videos, comunicación electrónica y…", *Op. Cit.*, pág. 4.

la monitorización del ordenador, los dispositivos de geolocalización y el control biométrico de los trabajadores.

1.- EL CONTROL AUDIOVISUAL DE LOS TRABAJADORES

Dentro de los sistemas de vigilancia que la empresa puede utilizar con ocasión de las NTIC, el control audiovisual resulta una figura clave[129]. El control audiovisual puede ser definido como aquel que el empresario ejercita valiéndose de dispositivos tecnológicos de vigilancia que permiten la grabación de imágenes y/o sonidos de los trabajadores[130]. Los micrófonos, las grabadoras de audio y las videocámaras son un claro ejemplo de estos dispositivos[131]. Si bien, cabe decir que la captación de la imagen del trabajador también puede ser practicada por detectives, cuyos servicios suelen ser contratados por el empresario con el fin de vigilar a los trabajadores más allá de su lugar y horario de trabajo[132].

El citado artículo 20.3 ET, confiere al empresario la potestad de emplear las medidas de vigilancia que estime como más oportunas sin establecer mayor concreción sobre este aspecto, salvo el debido respeto a la dignidad del trabajador. Así, en principio, el empresario puede acudir a sistemas de vigilancia como micrófonos o cámaras de video, con el fin de ejercer su derecho a controlar el cumplimiento de las obligaciones de sus empleados e informando debidamente a los representantes de los trabajadores[133]. Sin

[129] LLAMOSAS TRAPAGA, A. *Relaciones Laborales y nuevas…Op. Cit.,* pág. 139.
[130] Definición elaborada a partir de la noción de control empresarial que ofrece el artículo 20.3 ET y del término "videovigilancia" que da el Diccionario del Español Jurídico de la Real Academia Española. Disponible en: https://dej.rae.es/lema/videovigilancia (última visita: 10/03/2019).
[131] Véanse en este sentido las SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio, que examinan la licitud de las pruebas obtenidas con ocasión de la instalación de micrófonos y cámaras de video, respectivamente.
[132] ARIAS DOMÍNGUEZ, A.; SEMPERE NAVARRO, A. V., *Detectives en las Relaciones Laborales. Impacto de la Ley de Seguridad Privada (L 5/2014)*, Francis Lefebvre, Madrid, 2014, pág. 59. Véase también la STSJ Comunidad Valenciana 383/2000, de 3 de febrero, que permite el ejercicio de la videovigilancia fuera del lugar y tiempo de trabajo, con el fin de supervisar la conducta del empleado, cuando existan sospechas de que de esta pueda derivarse una transgresión de la buena fe contractual.
[133] EL artículo 64.5.f) ET impone al empresario la obligación de informar a los representantes de los trabajadores sobre las decisiones que tome en materia de control y organización del trabajo. Por su parte, el órgano de representación podrá emitir un informe de carácter no vinculante manifestando su opinión al respecto. En el mismo sentido, el artículo 10.3 de la Ley Orgánica de Libertad Sindical expone que los representantes sindicales de los trabajadores tendrán derecho a "ser oídos por la empresa previamente a la adopción de medidas de carácter colectivo que afecten a los trabajadores en general…". Asimismo, la AEPD también recoge la obligación informativa que tienen los empresarios para con los representantes en su Informe Jurídico núm. 0006/2009. Disponible en: https://www.aepd.es/informes/historicos/2009-0006.pdf (última visita: 10/03/2019).

embargo, como ya se ha mencionado anteriormente, este poder no es absoluto, y la legitimidad del sistema de control empleado estará relacionada con su debido respeto a los DDFF de los trabajadores[134].

Debido a la falta de normativa específica que existía en este sentido, los tribunales han sido los que, atendiendo a los casos concretos, han sentado las bases sobre la licitud y las limitaciones del control audiovisual de los trabajadores. Esta evolución jurisprudencial no se ha desarrollado de manera uniforme, hecho que permite distinguir entre dos etapas atendiendo a los DDFF que el Tribunal ha venido considerando como lesionados -como veremos-. De esta forma, mientras que en un principio la cuestión a enjuiciar era examinada a través del prisma del derecho a la intimidad del trabajador, más tarde, el TC introduce el derecho a la protección de datos como elemento decisivo en los conflictos sobre control audiovisual. En cualquier caso, la consecuencia de vulnerar un derecho u otro en la obtención de elementos de prueba será la misma, esto es, la no validez de la prueba causando que no pueda ser empleada en el juicio[135].

En este orden ideas, a continuación estudiaré la evolución de la cuestión que se viene tratando, a través de tres formas de control audiovisual, esto es: la captación de audio, las cámaras de videovigilancia y la contratación de detectives privados.

1.1.- La grabación de audio en el centro de trabajo

En términos generales, la grabación de las conversaciones de los trabajadores resulta un medio de control empresarial que puede parecer poco habitual, pues son escasas las resoluciones judiciales en este sentido. Sin embargo, existen ciertos ámbitos donde puede resultar una forma eficaz de vigilancia, como ocurre en las empresas de servicios telefónicos también conocidas como centro de atención de llamadas o *call center.*

En este sentido, resulta curioso que el primer pronunciamiento del TC respecto al uso de las NTIC como medio de control empresarial fuese precisamente sobre la instalación de micrófonos en el centro de trabajo. Así, la STC 98/2000, de 10 de abril,

[134] APARICIO ALDANA, R. K., *Derecho a la intimidad y… Op. Cit.*, págs. 138 y 139.
[135] GIMENO SENDRA. V., *Introducción al Derecho Procesal… Op. Cit.*, pág. 347. Véanse también las SSTC 98/2000, de 10 de abril, que declara nula la prueba de grabación de audio por vulnerar el derecho a la intimidad; y 29/2013, de 11 de febrero, que no admite la prueba de videovigilancia por lesionar el derecho a la protección de datos del trabajador.

constituye el punto de partida para una serie de resoluciones judiciales que examinan la constitucionalidad de los mecanismos de control audiovisual en el ámbito laboral[136].

Dicha sentencia estudia el caso de la empresa Casino de La Toja que, contando con un sistema de videovigilancia, instaló micrófonos en zonas puntuales sin que existieran sospechas previas de posibles irregularidades por parte de los trabajadores. Estos dispositivos de grabación no estaban ocultos y permitían a la empresa registrar las conversaciones de empleados y clientes de manera indiscriminada.

Ante estos hechos, el TC aplica el test de proporcionalidad resolviendo que la medida empresarial vulneraba el Derecho Fundamental a la intimidad de los trabajadores por ser desproporcionada, pues la grabación de las conversaciones resulta una intromisión a la vida privada tanto de los trabajadores como a la de los clientes. Apunta la sentencia que el registro simultáneo de imagen y sonido es especialmente invasivo para la intimidad de los trabajadores y que dicha técnica solo será admisible cuando sea imprescindible para la empresa y no exista otro mecanismo menos gravoso para los DDFF del trabajador[137].

En este sentido, "para dilucidar en cada caso concreto si esos medios de vigilancia y control respetan el derecho a la intimidad de los trabajadores", el intérprete constitucional establece como relevante el lugar concreto que registra el dispositivo, si la instalación se hace de manera masiva o puntual, la visibilidad u ocultación del sistema de vigilancia, la finalidad de la medida, el tipo de actividad desarrollada en la empresa, y el conocimiento del empleado y/o sus representantes de la existencia de los dispositivos de control[138]. Es decir, el hecho de que la normativa regule expresamente la prohibición de herramientas de vigilancia (tales como grabadoras de audio o cámaras de video) en vestuarios, baños y zonas de descanso ante la posibilidad de atentar contra la vida íntima

[136] Así lo expresa CAVAS MARTÍNEZ en su ponencia "Los Derechos Fundamentales y las Libertades Públicas en el ámbito Laboral", impartida en el marco del *I Seminario del Área de Derecho Laboral y de la Seguridad Social*, el 23 de febrero de 2015 en la Universidad Miguel Hernández de Elche (Alicante), cuando afirma que "la STC que en primer lugar -con algún precedente, pero la más importante- se pronunció sobre la validez de las grabaciones audiovisuales en el entorno del centro de trabajo fue la STC 98/2000, de 10 de abril…". Disponible en: https://www.youtube.com/watch?v=fECK5u0FO6A (última visita: 15/03/2019).

[137] La STC 98/2000, citando a su vez la STSJ Cataluña de 25 de abril de 1994, se pronuncia a este respecto expresando que las cámaras de videovigilancia satisfacen el interés de la empresa y que "si se añadiera el control auditivo al visual, la fiscalización sería completa, pero asimismo sería completa la vulneración del derecho a la intimidad personal del trabajador (…) la sujeción del trabajador a una vigilancia auditiva es una agresión intolerable si no existe una excepcional razón técnica, al suponer una compresión absoluta de un derecho de rango constitucional".

[138] Téngase en cuenta que el TC se expresa aquí en términos generales cuando habla de sistemas audiovisuales de control, extendiendo así su pronunciamiento a las medidas de videovigilancia entendidas como la captación de la imagen de los trabajadores (que serán tratadas más adelante).

de los trabajadores[139], no significa que la intimidad del trabajador no pueda verse vulnerada en cualquier otro espacio del lugar de trabajo, si bien, debe cumplirse el principio de proporcionalidad[140].

Otro ejemplo del conflicto que surge en cuanto a esta materia podemos encontrarlo en la STS, sala de lo Social, de 5 de diciembre de 2003 (núm. rec. 52/2003), que examina la validez de la grabación de conversaciones de los trabajadores en una empresa dedicada al márketing telefónico.

En este caso, la empresa registraba de manera aleatoria conversaciones telefónicas entre los asesores comerciales y sus respectivos clientes[141]. La medida de control era conocida por los empleados y tenía por objeto detectar posibles errores en las técnicas de venta para mejorar la calidad del servicio ofertado por la empresa. Además, el centro de trabajo disponía de zonas de descanso con teléfonos no intervenidos que los trabajadores podían usar para fines personales.

El TS determinó que las escuchas eran necesarias, puesto que no existía un medio de control menos intrusivo para la vida íntima del empleado capaz de obtener el fin perseguido por la empresa, y que la medida resultaba idónea y equilibrada, pues no producía perjuicio alguno para los DDFF de los trabajadores ya que la empresa disponía de teléfonos para uso particular. Por lo que el Tribunal resuelve que no existió una transgresión del artículo 18.1 CE, pues la medida superaba el test de la proporcionalidad y por tanto, era lícita.

Ambas resoluciones (STC 98/2000 y STS de 5 de diciembre de 2003) se pronuncian siguiendo la misma línea doctrinal, evidenciando que la aplicación del test de proporcionalidad -atendiendo a las circunstancias de cada caso- es lo que determina si una medida empresarial se ajusta a derecho o no. Por tanto, para saber si la medida de control de audio lesiona el Derecho Fundamental a la intimidad, habrá que observar si el dispositivo de vigilancia es capaz de conseguir el fin perseguido por la empresa (juicio

[139] No obstante, el TSJ de Madrid ha permitido la instalación de videocámaras en la zona de comedor de una empresa cuando la baja calidad de la grabación no permite la identificación de los trabajadores (STSJ Madrid 412/2006, de 14 de junio). En el mismo sentido, véanse las SSTSJ Cataluña de 24 de abril de 2007; y Murcia 162/2003, de 3 de febrero que permiten la instalación de cámaras en las zonas de acceso a los vestuarios siempre que no graben su interior.

[140] La STC 98/2000, de 10 de abril, establece que los trabajadores siguen teniendo derecho a la protección de su vida íntima incluso durante el desarrollo de la prestación laboral. Esta afirmación matiza la anterior doctrina (véanse las SSTC 202/1999, de 8 de noviembre; 142/1993, de 22 de abril; y 180/1987, de 12 de noviembre) en la que se determinaba que, en principio, la vida privada no tenía cabida dentro del ámbito de las RRLL.

[141] Concretamente, las escuchas se realizaban sobre el 0,5% de las llamadas, tal y como expone el antecedente de hecho 4º de la STS de 3 de diciembre de 2003.

de idoneidad); si no existe una medida menos restrictiva de los DDFF de los trabajadores que cumpla con el mismo fin (juicio de necesidad); y si la medida es equilibrada, en el sentido de derivarse de ella más ventajas para el interés general que perjuicios para los derechos de los trabajadores (juicio de proporcionalidad en sentido estricto)[142].

El test de proporcionalidad se aplica aquí en relación con el derecho a la intimidad de los trabajadores. No obstante, como veremos a lo largo de este trabajo, el principio de ponderación seguirá siendo invocado en numerosos pronunciamientos sobre el conflicto que surge por el uso de medidas tecnológicas de control empresarial en el ámbito laboral, ya sea desde el punto de vista del derecho a la intimidad o, a través de la perspectiva del derecho a la protección de datos.

En cuanto a la normativa específica sobre grabaciones de audio, el artículo 7 de la Ley de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen dispone que, de manera general, "tendrán la consideración de intromisiones ilegítimas: 1. El emplazamiento en cualquier lugar de aparatos de escucha (…) o de cualquier otro medio apto para grabar reproducir la vida íntima de las personas; 2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción"[143].

Asimismo, la LOPDGDD también hace referencia de manera expresa a este conflicto en su artículo 89, que introduce una serie de condiciones que todo empleador ha de cumplir para implantar medidas legítimas de control basadas en la grabación de audio: primero, la actividad laboral que desarrolle la empresa deberá suponer un riesgo relevante "para la seguridad de las instalaciones, bienes y personas" en el centro de trabajo; segundo, la medida de control respetará los principios de proporcionalidad y de intervención mínima; tercero, los trabajadores (y sus representantes, si los hubiere) deberán ser informados con "carácter previo, y de forma expresa, clara y concisa" acerca de la medida; y cuarto, queda prohibida la grabación de audio en zonas de ocio o descanso pertenecientes a la empresa. Del mismo modo, la LOPDGDD regula la eliminación de las

[142] En este sentido, véanse las SSTC 207/1996, de 16 de diciembre; 55/1996, de 28 de marzo; y 66/1995, de 8 de mayo. Véase también DESDENTADO BONETE, A.; MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y… Op. Cit.,* págs. 20 – 24.

[143] Este precepto hace referencia, a su vez, al artículo 2 de la Ley de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que excluye "la existencia de intromisión ilegítima (…) estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso".

conversaciones almacenadas por sistemas audiovisuales de control indicando que estas deben realizarse, como norma general, en el plazo de un mes desde su registro. Sin embargo, en caso de que las grabaciones acrediten "la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones" podrán ser conservadas debiendo ser puestas a disposición de la autoridad competente en el plazo de setenta y dos horas desde que se tenga conocimiento[144].

Ciertamente, este es un análisis concreto sobre el empleo de dispositivos de captación de audio como control de los trabajadores, sin embargo, las resoluciones citadas a continuación seguirán sentando las bases sobre el uso de sistemas de control audiovisual. Es decir, la doctrina en relación con la videovigilancia también será de aplicación al control a través de grabación de audio, en tanto en cuanto, ambas son técnicas de control audiovisual.

1.2.- La videovigilancia de los trabajadores

El control visual de los trabajadores puede ser realizado a través de la técnica de videovigilancia que supone la supervisión a través de la captación y/o grabación de imágenes con cámaras, fijas o móviles[145]. El uso de este medio de control sigue creciendo cada año en el mundo empresarial, entre otros motivos, por resultar más económico que la vigilancia a través de personal cualificado[146].

Al igual que ocurre con la vigilancia de los trabajadores a través de sistemas de control de sonidos, el control visual está permitido en virtud del derecho de supervisión del empresario. Sin embargo, existen ciertos espacios vetados para el uso de sistemas de videograbación como vestuarios, baños, comedores, o locales dedicados a la actividad sindical[147].

Siguiendo con la evolución jurisprudencial iniciada con la STC 98/2000, encontramos la STC 186/2000, de 10 de julio, que examina la licitud de la instalación de

---

[144] Artículo 22.3 LOPGDGG.

[145] Véase la ficha práctica de videovigilancia de la AEPD sobre información general disponible en: https://www.aepd.es/media/fichas/ficha-videovigilancia-folleto-general.pdf (última visita: 01/05/2019).

[146] GOÑI SEIN, J.L., *La videovigilancia empresarial y… Op. Cit.*, págs. 17 – 18. Véase también BLÁZQUEZ AGUDO, E. M., *Aplicación práctica de la protección… Op. Cit.*, pág. 105.

[147] Véase la Guía de Videovigilancia de la AEPD, pág. 35. Disponible en: https://www.prevent.es/Documentacion/guia_videovigilancia.pdf (última visita: 18/05/2019). En el mismo sentido, véanse las SSTSJ Madrid de 14 de abril de 2009; Castilla y León 1479/2006, de 18 de septiembre; y Madrid 2155/2000, de 14 de septiembre.

un sistema de videovigilancia, en su relación con el derecho a la intimidad de los trabajadores.

En concreto, la empresa instaló cámaras de video en la zona de caja ante las sospechas previas de graves irregularidades por parte de algún trabajador. La instalación se realizó de manera oculta y supuso una medida temporal. Este hecho no fue puesto en conocimiento de los trabajadores ni del Comité de Empresa. Así, a través de las grabaciones, la empresa pudo constatar que un empleado sustraía diferentes cantidades de dinero de manera reiterada, razón por la cual fue despedido de manera disciplinaria.

Ante esto, el TC declaró que las sospechas previas justificaban la medida de control empleada y que, además, la instalación cumplía con los tres requisitos del test de proporcionalidad. En cuanto a la falta de información sobre la medida, este hecho queda plenamente justificado, ya que una advertencia previa no habría permitido descubrir qué ocasionaba el grave descuadre contable. Así, la STC concluyó que el sistema de videovigilancia no lesionaba el derecho a la intimidad de los trabajadores y, por tanto, las grabaciones eran aceptadas como elemento de prueba para justificar el despido disciplinario del trabajador.

Por tanto, en relación con el uso de videovigilancia y el derecho a la intimidad de los trabajadores, se puede afirmar lo siguiente: primero, el derecho a la intimidad consagrado en el artículo 18.1 CE cabe ser invocado en el ámbito de las RRLL, pero no es absoluto, pudiendo ser limitado; segundo, los medios de control audiovisual afectan al derecho a la intimidad de los trabajadores (sin entrar a valorar la posible incidencia de la medida sobre otro Derecho Fundamental); tercero, la instalación subrepticia de mecanismos de control audiovisual lesiona el artículo 18.1 CE, excepto si existen sospechas fundadas sobre la existencia de ilícitos laborales graves. Estas sospechas justifican también el incumplimiento del deber de información que tiene el empresario para con los representantes de los trabajadores; y cuarto, el triple examen de proporcionalidad será de aplicación -en atención a las circunstancias de cada caso- con el fin de conocer si las medidas empresariales violan o no el Derecho Fundamental a la intimidad[148].

[148] En este sentido, APARICIO ALDANA dice que el uso de videovigilancia sin informar a trabajadores ni a sus representantes se encuentra tutelado por el derecho a la libertad de empresa del artículo 38 CE cuando es necesario adoptar esta medida de manera extraordinaria debido a sospechas de un incumplimiento grave. Sin embargo, en caso de no existir indicios, la decisión empresarial de implantar un sistema de grabación en la empresa deberá seguir los cauces normales de publicidad, en *Derecho a la intimidad y… Op. Cit.*, pág. 150.

Esta doctrina sería modificada años más tarde, cuando la línea jurisprudencial seguida por el TC comenzó a valorar la licitud de las medidas empresariales de videovigilancia no solo desde la perspectiva del derecho a la intimidad personal y familiar, sino también, a través del prisma de la protección de datos de carácter personal[149]. A partir de este momento, el TC pasó a cuestionar si la captación de la imagen del trabajador, en la medida en que esta supone un dato de carácter personal, lesiona o no el derecho a la protección de datos[150].

La STC 29/2013, de 11 de febrero, examinó la validez de las imágenes que las cámaras de seguridad de la Universidad de Sevilla captaron y que fueron utilizadas como medio de prueba para acreditar un incumplimiento laboral. Concretamente, las cámaras eran dispositivos fijos instalados en las zonas de acceso a los edificios de la universidad cuyo fin era contribuir a la seguridad. Los dispositivos eran visibles, estaban debidamente señalizados y contaban con las autorizaciones administrativas necesarias según la AEPD[151]. Ante la sospecha de incumplimientos en el horario laboral por parte de un empleado, el Director de Recursos Humanos decidió utilizar las cámaras de seguridad instaladas en la entrada del centro de trabajo (un edificio del campus universitario) con el fin de acreditar dicho ilícito laboral. A través de las imágenes captadas, la empresa pudo constatar cómo un trabajador incumplía su horario de trabajo de manera reiterada (entre otras irregularidades), por lo que fue sancionado disciplinariamente con la suspensión de empleo y sueldo por infracciones muy graves. Este nuevo uso fiscalizador de las grabaciones no fue puesto en conocimiento de los trabajadores ni de sus representantes.

---

[149] Según expone ARRABAL PLATERO en "La videovigilancia laboral…", *Op. Cit.*, pág. 11, el ATS 28/2007, de 11 de enero, es el pronunciamiento que comienza a relacionar la técnica de videovigilancia con el derecho a la protección de datos.

[150] Así lo explica CAVAS MARTÍNEZ en su ponencia "Los Derechos y Libertades Fundamentales en materia laboral", realizada en el marco del I Seminario del Área de Derecho del Trabajo y la Seguridad Social y que tuvo lugar el 23 de febrero de 2015 en la Universidad Miguel Hernández de Elche (Alicante). Disponible en: https://www.youtube.com/watch?v=fECK5u0FO6A (última visita: 15/03/2019). Asimismo, ARRABAL PLATERO afirma que "tanto el Tribunal Constitucional, cuanto el Tribunal Supremo se han servido del prisma de la protección de datos para censurar las grabaciones de videovigilancia como prueba en un proceso judicial en el que se discutían medidas laborales de carácter disciplinar", en "La videovigilancia laboral…", *Op. Cit.*, pág. 13.

[151] La AEPD establece que, si del uso de sistemas de videovigilancia y el tratamiento de sus datos, se deriva la creación de ficheros ("conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"), esto debe ser comunicado de manera previa a la AEPD, que procederá a la inscripción de la empresa en el Registro General de la AEPD. Véase en este sentido la ficha práctica sobre videovigilancia y control empresarial y el cartel de "Zona Videovigilada" que exige la AEPD. Disponibles, respectivamente, en: https://www.aepd.es/media/fichas/ficha-videovigilancia-control-empresarial.pdf y https://www.aepd.es/media/fichas/cartel-videovigilancia.pdf (última visita: 18/05/2019).

En este contexto, el TC concluyó que la medida de control empresarial no lesionaba el derecho a la intimidad del trabajador, ya que el uso que la universidad había dado a la videovigilancia respetaba el principio de proporcionalidad. En este aspecto, el TC sigue el criterio expuesto en la STC 186/2000 justificando el control oculto con el fin perseguido por la empresa, esto es, confirmar la existencia de un incumplimiento laboral (téngase en cuenta que, a pesar de que las cámaras están señalizadas, el nuevo uso que la empresa otorga a los dispositivos de video no fue puesto en conocimiento de los trabajadores, de ahí que se hable de "control oculto").

Sin embargo, la medida de videovigilancia sí era contraria al derecho amparado por el artículo 18.4 CE con causa en la falta de información sobre la finalidad de control laboral de las cámaras de seguridad. Pues, en la medida en que la imagen del trabajador supone un dato de carácter personal, la actuación empresarial sobre dichos datos sería considerada como una actividad de tratamiento y, a su vez, el almacenamiento de las imágenes supondría la creación de un fichero informático[152].

Con esta afirmación, la STC 29/2013, de 11 de febrero, continúa con la doctrina ya fijada por la STC 292/2000, de 30 de noviembre, que determinó que la autotutela informativa se constituye como un Derecho Fundamental autónomo entendiendo que el derecho de información es un complemento necesario del derecho consagrado en el artículo 18.4 CE[153]. Con base en esta resolución, la citada STC 29/2013 rechazó la validez del medio de prueba obtenido a través de las cámaras de videovigilancia por vulnerar el derecho a la protección de datos de carácter personal, y por ende, las sanciones disciplinarias impuestas al trabajador eran nulas[154].

Como vemos, el TC introduce una serie de condiciones adicionales necesarias para la validez de la videovigilancia que giran en torno al deber de información que trae

[152] Según el artículo 4 RGPD son datos personales: "toda información sobre una persona física identificada o identificable"; el tratamiento de datos es: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"; y el fichero es: "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

[153] La STC 292/2000, de 30 de noviembre, establece que la función del derecho a la protección de datos es garantizar al ciudadano el control sobre el uso de sus datos personales, por lo que "si el afectado desconoce qué datos son los que poseen terceros, quienes lo poseen y con qué fin" de nada sirve su derecho de controlar sus propios datos.

[154] El fallo cuenta con un voto particular que discrepa de la interpretación establecida por el resto de magistrados. En dicho voto se considera que la medida de control no lesiona el derecho a la protección de datos y que el test de la proporcionalidad ha de ser aplicado en este caso.

consigo el derecho a la protección de datos personales. De este modo, la sentencia resuelve que: la información debe ser "previa, expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral"; la exclusión de la necesidad de consentimiento en el ámbito de las relaciones laborales no exime del cumplimiento del deber informativo[155]; la visibilidad de las cámaras y/o la colocación de carteles normativos no son suficientes para cumplir con la obligación informativa del empleador; el trabajador puede considerar que existen expectativas razonables de confidencialidad si no ha sido informado de la finalidad de las medidas de videovigilancia empresarial en las condiciones que determinan en la propia sentencia; y no se permite, en ningún caso, la videovigilancia encubierta[156].

A pesar de esta doctrina, posteriores pronunciamientos aceptarían los sistemas de videovigilancia instalados de manera subrepticia sin que la ausencia de información supusiera automáticamente la lesión del derecho a la protección de datos. En este sentido, si la videovigilancia era una medida puntual y temporal a la que el empresario acudía ante sospechas previas, cabría la ocultación es de este medio de control. Si bien, tal circunstancia habría de ponderarse aplicando el test de la proporcionalidad[157].

Avanzando en la evolución de la jurisprudencia sobre videovigilancia, destaca la STC 39/2016, de 3 de marzo, por dar un nuevo giro delimitando el alcance del derecho a la información de los trabajadores.

El TC enjuició la validez de las grabaciones de videovigilancia como elemento probatorio en el despido disciplinario una empleada de la empresa Bershka. La tienda, siendo conocedora de irregularidades contables, contrató a una compañía de seguridad que instaló un sistema de cámaras que grababa la zona de caja. A pesar de que este hecho no fue puesto en conocimiento de los trabajadores ni del Comité de Empresa, sí que se colocó la pertinente señalización que exige la AEPD en un lugar visible. Las grabaciones

[155] La anterior normativa de protección de datos contenía un precepto (artículo 6.2 de la Ley de Protección de Datos de 1999) que excluía la necesidad de consentimiento ante el tratamiento de datos en el ámbito de las RRLL.

[156] Entre las sentencias que aplican dicha doctrina, se encuentra la STS de 13 de mayo de 2014 (núm. rec. 1685/2013), que declaró la nulidad de la prueba obtenida a través de un circuito cerrado de televisión instalado en la zona de caja de un supermercado por vulnerar el derecho a la protección de datos de la empleada. Las cámaras de videovigilancia eran visibles, por lo que los trabajadores conocían su existencia y el supermercado informó al Comité de Empresa de que el fin de las cámaras era la seguridad ante posibles robos de los clientes. A través de las grabaciones, la empresa constató irregularidades por parte de una trabajadora que realizaba cargos y abonos indebidos.

[157] Véanse en este sentido la sentencia del Juzgado de lo Social núm. 3 de Elche, de 14 de mayo de 2014, y la STSJ Cataluña de 11 de marzo de 2013 que distinguen entre los sistemas de videovigilancia fijo de las que el control se realiza puntualmente y de manera limitada en el tiempo.

permitieron a la empresa acreditar que una empleada, de forma habitual, se apropiaba de dinero en efectivo que sustraía de la caja registradora.

En este contexto, el TC resuelve entendiendo que la empresa cumplió con su deber de información y, por tanto, no se vulneró el derecho a la protección de datos de la trabajadora. El intérprete constitucional razona que la dependienta se encontraba en disposición de conocer la existencia de las cámaras, pues el sistema de videograbación era visible y el cartel ubicado en la tienda informaba de este hecho. Asimismo, la prueba obtenida a través de las cámaras de video no lesionó el derecho a la intimidad ya que la considera justificada (basándose en las razonables sospechas de la empresa) y superó el juicio de proporcionalidad[158].

Cabe destacar la diferenciación que ofrece el TC atendiendo al momento en que se lleva a cabo la videovigilancia distinguiendo entre dos situaciones: por un lado, si el sistema de videovigilancia es fijo y supone una medida permanente en el tiempo, el empresario deberá informar a los trabajadores; por el contrario, si las cámaras constituyen un hecho puntual y temporal al que el empresario acude ante fundadas sospechas de irregularidades laborales, la medida de control deberá respetar la intimidad de los trabajadores y superar el test de proporcionalidad para ser considerada lícita[159].

En este orden de ideas, se deduce que el deber de información continúa siendo un aspecto relevante en cuanto a la validez de las medidas de control empresarial. Sin embargo, esta obligación se torna más flexible, dado que la mera colocación del distintivo informativo que exige la AEPD exime al empresario de poner en conocimiento de los trabajadores la finalidad de la medida de control. De esta manera, no cabe la lesión del artículo 18.4 CE y el TC se centrará en determinar si el sistema de videovigilancia transgrede el derecho a la intimidad de los trabajadores, ponderando la medida sobre la base del test de proporcionalidad.

En consecuencia, se evidencia que esta corriente sitúa en un mismo nivel tanto el poder de control empresarial, como los DDFF de los trabajadores, contradiciendo así, la idea de supremacía de los DDFF sobre la que se asienta nuestro ordenamiento jurídico.

[158] Según el TC, no resulta necesario "especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control", STC 39/2016, FJ 4º. Véanse las SSTS de 2 de febrero de 2017, de 31 de enero de 2017 y de 7 de julio de 2016 que aplican el deber de información de carácter flexible en el mismo sentido.
[159] GONZÁLEZ GONZÁLEZ, C., "Control empresarial de la actividad laboral mediante video vigilancia y colisión con los derechos fundamentales del trabajador. Novedades del Proyecto de Ley Orgánica de protección de datos derechos digitales", *Revista Aranzadi Doctrinal*, núm.4, 2019, pág. 21.

Vista la doctrina expuesta por SSTC 29/2013 y 39/2016, surge una cuestión que resulta de relevancia en la materia que nos ocupa, esta es: ¿se está permitiendo que pruebas digitales capaces de acreditar delitos no sean tomadas en consideración en aras de garantizar a los trabajadores el derecho a disponer y controlar sus datos personales?[160].

En este sentido, se ha pronunciado el TEDH con su sentencia de 9 de enero de 2018 en el asunto López Ribalda y otras v. España, cuyo conflicto gira en torno a la licitud del sistema de videovigilancia que una empresa instaló ante sospechas previas de irregularidades por parte de algunos empleados[161].

La empresa (un supermercado) colocó cámaras en dos lugares, unas en la zona de entrada y salida del supermercado, y las otras en la zona de caja. Los dispositivos que grababan la zona de acceso al supermercado eran visibles, y la empresa había informado a los trabajadores y sus representantes de este hecho. Por el contrario, las cámaras que captaban imágenes en la zona de caja estaban ocultos y su instalación no había sido puesta en conocimiento de los empleados. El visionado de las imágenes permitió comprobar que cinco empleadas sustraían productos de manera reiterada, hecho por el que fueron despedidas de manera disciplinaria.

Los despidos fueron impugnados ante la Jurisdicción Social argumentando que la actuación empresarial vulneraba el derecho a la intimidad y el derecho a la protección de datos de las trabajadoras. Sin embargo, tanto el Juzgado de lo Social como el TSJ de Cataluña califican los despidos como procedentes[162]. Del mismo modo, el TC no admite recurso de amparo en este caso.

El litigio alcanza al TEDH que resuelve que la prueba obtenida con ocasión de un medio de vigilancia oculto vulnera el artículo 8 CEDH sobre el respeto a la vida privada y familiar[163]. La STEDH asevera que la videovigilancia encubierta de los trabajadores supone "una intrusión considerable en la vida privada y una ilegítima privación del derecho a disponer de sus propios datos". Según el TEDH, las trabajadoras tenían derecho

[160] Tanto la STC 29/2013 como la STC 39/2016 cuentan con un voto particular en contra de la resolución dictada por el Tribunal, hecho que refleja la controversia existente en torno al deber de información y la licitud de la videovigilancia encubierta.
[161] Sentencia disponible en: https://www.icav.es/bd/archivos/archivo11428.pdf (última visita: 20/05/2019).
[162] Véase la sentencia del Juzgado de lo Social núm. 1 de Granollers, de 20 de enero de 2010, y la STSJ Cataluña 1481/2011, de 24 de febrero.
[163] El artículo 8 CEDH establece que: "1.Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia; 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

a ser informadas sobre la existencia y finalidad de la medida de control en los términos recogidos en la Ley Orgánica de Protección de Datos de Carácter Personal, es decir, con antelación a su aplicación, de forma expresa, precisa e inequívoca[164]. En consecuencia, la falta de información provocó que las empleadas tuvieran unas expectativas razonables de confidencialidad sobre sus actos. Asimismo, estima el Tribunal que no cabe justificar la actuación empresarial en la existencia de sospechas en este caso, pues las cámaras grababan a todos los trabajadores, durante toda la jornada laboral y de manera prolongada en el tiempo[165].

Como se observa, el TEDH sigue la corriente establecida por la STC 29/2013 basada en el conocimiento previo de la instalación del sistema de videovigilancia y su finalidad concreta como requisito imprescindible en la determinación de la validez de la medida empresarial. Así, el Tribunal de Estrasburgo está marcando las pautas a seguir en cuanto a la problemática sobre la información previa a los trabajadores, lo que supone, a su vez, la desautorización de lo establecido en la STC 39/2016, de 3 de marzo[166].

Esta tesis garantista se ve reforzada por el RGPD que establece que la obligación empresarial de información debe ser rigurosa y, en todo caso, deberá cumplirse en el uso de medidas de control de los trabajadores que supongan la creación de un fichero informático[167]. De igual modo, el Reglamento reconoce a todo afectado el derecho de acceso, rectificación, cancelación, olvido y portabilidad sobre sus datos personales (en este caso imágenes). La persona responsable del tratamiento de los datos debe facilitar el cumplimiento de estos derechos, para lo cual debe informar de manera previa, clara y concisa sobre estas cuestiones[168]. Los trabajadores tienen derecho a acudir a la AEPD para presentar una reclamación si el tratamiento de sus datos personales no se ajusta a la

[164] Téngase en cuenta que la normativa sobre protección de datos en vigor durante los hechos que narra la sentencia es el RGPD y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[165] La STEDH cuenta con un voto particular pronunciándose en sentido contrario que opina que un tratamiento riguroso del deber informativo puede amparar conductas de los trabajadores contrarias a derecho.

[166] Esta "desautorización" es posible ya que, en virtud del artículo 10.2 CE, los dictámenes del TEDH resultan de aplicación directa en los países miembros de la Unión Europea.

[167] Según el RGPD un fichero es "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica". Es posible que un sistema de videovigilancia no genere un fichero informático si no almacena las imágenes que capta y su única función es proyectarlas en un monitor. En este sentido, BLÁZQUEZ AGUDO establece que en estos casos los trabajadores deben ser informados de la existencia del sistema de control, si bien, no es necesario poner en su conocimiento los derechos específicos que poseen sobre su imagen (puesto que estas no permanecen de ninguna forma), en *Aplicación práctica de la… Op. Cit.,* pág. 193.

[168] Véase en este sentido la pág. 6 de la "Guía para el cumplimiento del deber de informar" elaborada por la AEPD en colaboración con las Agencias de Protección de Datos del País Vasco y Cataluña. Disponible en: https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf (última visita: 21/05/2019).

normativa, sin perjuicio de posteriores reclamaciones ante los juzgados o posibles indemnizaciones por daños y perjuicios[169]. Sin embargo, el consentimiento del trabajador para recabar sus datos personales solo será necesario si el empresario tiene un objetivo distinto del laboral, pues esta autorización se presume como realizada en virtud de un contrato de trabajo[170].

El RGPD también recoge el principio de proporcionalidad como límite al tratamiento de los datos personales. Concretamente, el artículo 5.1.c) RGPD expresa que los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)". El artículo 6 expone que para que el tratamiento de datos sea lícito deberá (entre otras condiciones) ser "necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales".

Así las cosas, con la entrada en vigor de la nueva normativa en materia de protección de datos se produce una vuelta a la doctrina que abogaba por un deber de información flexible. Así, el artículo 89.1 LOPDGDD recoge una importante excepción al derecho de autotutela informativa "en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos", en cuyo caso, el deber de información se entenderá cumplido con la colocación del distintivo que exige la AEPD[171]. Se evidencia, por tanto, una clara contradicción entre la legislación española y la doctrina y norma europea.

Este conflicto encuentra su solución en el Tratado de Funcionamiento de la Unión Europea pues, en virtud del artículo 288, los reglamentos europeos son de alcance general a toda la Unión Europea, obligatorios y directamente aplicables en los Estados miembros. Así, el RGPD prima sobre la normativa interna que entre en contradicción con su contenido. Del mismo modo, como hemos visto, las sentencias del TEDH son vinculantes

[169] Véanse los artículos 77, 79, 82 y 146 RGPD. En este sentido, BLÁZQUEZ AGUDO razona que la creación de un espacio en internet donde la empresa informe a sus trabajadores sobre el tratamiento de sus datos (y otros aspectos relacionados) resultaría de gran utilidad, puesto que permitiría a los trabajadores tener un acceso permanente a esta información y supondría a las empresas un ahorro en costes para el cumplimiento de sus obligaciones en materia de protección de datos, en *Aplicación práctica de la… Op. Cit.,* págs. 105 y 106.

[170] Véase la Resolución núm. 330/2000 de la AEPD que trae causa en el uso de las imágenes de los trabajadores captadas a través de cámaras de video con el objetivo de publicitar a la empresa, hecho que va más allá de la relación contractual.

[171] Mismo criterio que seguía la STC 39/2016, de 3 de marzo.

al Estado español y directamente aplicables. Por tanto, en materia de videovigilancia, no cabe invocar la legitimidad de medidas de control subrepticias en vista del artículo 89.1 LOPDGDD. De hacerlo, los tribunales deberán inaplicar la ley española pues "en ningún caso una ley interna puede rebajar las exigencias del deber informativo que establece el RGPD"[172].

La sentencia del Juzgado de lo Social núm. 3 de Pamplona 52/2019, de 18 de febrero es un claro ejemplo de esta afirmación. Este pronunciamiento resulta de gran relevancia tanto por el momento en que se dicta (en un contexto de adaptación a la LOPDGDD), como por el análisis sobre la validez de la prueba que realiza el magistrado donde repasa las características más importantes de la jurisprudencia sobre videovigilancia, así como del RGPD y la LOPDGDD[173].

La sentencia trae causa el despido improcedente de un trabajador por golpear a otro empleado fuera de la jornada laboral. El demandante discutió con un superior respecto a una orden de trabajo, persiguiéndole por el centro de trabajo y espetándole que le esperaría a la salida. Tras la jornada laboral, ambos trabajadores se enzarzan en una pelea en el parking de la empresa, siendo separados por otro empleado quien presenció lo sucedido. La empresa disponía de un sistema de videovigilancia (con el distintivo que exige la AEPD) que grabó los hechos.

El magistrado declara nula la prueba basada en las grabaciones de la pelea por no cumplir con las exigencias informativas que fija el RGPD. Esto es, poner en conocimiento de los trabajadores la existencia del sistema de videovigilancia, así como la finalidad que tiene, incluyendo la posibilidad de sancionar si captan infracciones laborales.

No obstante, la sentencia resuelve calificando el despido como procedente, pues, a pesar de que la grabación vulneró el derecho a la protección de datos del demandante, la agresión pudo ser confirmada a través de pruebas documentales y testificales.

Como vemos, esta resolución de Pamplona se pronuncia conforme a la doctrina del TEDH y bajo el mismo razonamiento de primacía de las normas europeas que ha sido expuesto anteriormente. Así, establece que toda actuación empresarial solo es válida si supera el triple juicio de la proporcionalidad y que el deber informativo debe ser previo,

[172] GONZÁLEZ GONZÁLEZ, C., "Control empresarial de la actividad…", *Op. Cit*., pág. 32.
[173] El titular del Juzgado de lo Social núm. 3 de Navarra, GONZÁLEZ GONZÁLEZ, establece en esta sentencia que los cinco "hitos más característicos" en cuestión de control visual son: la doctrina constitucional hasta las SSTC 29/2013 y 39/2016; el deber informativo en la doctrina de las SSTC 29/2013 y 39/2016; c) La prohibición de la videovigilancia encubierta en la doctrina de la STEDH, de 9 de enero de 2018, (caso "López Ribalda y otras v. España); la incidencia del RGPD; y el deber informativo en la LOPDGDD.

expreso, claro e inequívoco sobre la existencia de los dispositivos, la finalidad que tienen y la posibilidad que de sus grabaciones se deriven sanciones. En relación con las medidas de control empresarial ocultas o no informadas, concluye la sentencia que, ante sospechas de ilícitos laborales, el empresario debería recurrir al auxilio judicial para interponer la pertinente denuncia y así solicitar la práctica de la videovigilancia en su empresa.

Visto todo lo anterior, resulta evidente que la protección de datos de carácter personal es un derecho cuya incidencia en las RRLL cada vez es mayor. Asimismo, el control empresarial basado en la videovigilancia resulta especialmente problemático, sobre todo si los dispositivos constituyen un medio encubierto. En todo caso, el criterio a seguir es el deber informativo riguroso que fija el RGPD, esto es, de manera previa, expresa, clara e inequívoca sobre la medida que va a aplicar el empresario y su finalidad (no pudiendo atribuir un fin distinto del informado). Si bien, esta "regla" podría cambiar, pues la STEDH de 9 de enero de 2018 se encuentra actualmente en revisión por la Gran Sala.

1.3.- Los detectives privados en el ámbito laboral

Hasta ahora, la jurisprudencia analizada examinaba situaciones en las que los sistemas de control informático eran instalados en el centro de trabajo, valorando en algunos casos si dicho instrumento de grabación es fijo y permanente o, por el contrario, se trata de una medida puntual y limitada en el tiempo. Los tribunales también han estudiado la licitud de los medios de control encubiertos, resolviendo -como hemos visto- que toda medida será legítima si el deber de información se cumple con rigor tal y como establece el TEDH y el RGPD.

En este punto, cabe plantearse si los empresarios pueden extender su poder de control empresarial más allá de la prestación laboral, lo que traería a colación el uso de la figura del detective privado como herramienta de vigilancia empresarial. Pues bien, el control de los trabajadores fuera del lugar y tiempo de trabajo se ha venido permitiendo por la jurisprudencia siempre que la conducta del empleado pueda afectar a su prestación laboral y suponer una transgresión de la buena fe contractual, entre otras condiciones[174]. Así, los detectives privados se han convertido en una figura muy interesante dentro del

[174] Véase en este sentido la STSJ Comunidad Valenciana 383/2000, de 3 de febrero, que permite la videovigilancia practicada por un detective privado fuera del lugar de trabajo y horario laboral de un empleado para verificar su estado de enfermedad. En el mismo sentido se pronuncian ARIAS DOMÍNGUEZ, A.; SEMPERE NAVARRO, A. V., *Detectives en las Relaciones Laborales… Op. Cit.,* pág. 59.

proceso judicial, y más concretamente en el ámbito laboral, pues suponen una herramienta de control audiovisual muy útil para el empresario[175].

El detective privado es, en palabras de la Real Academia Española, un "policía particular que practica investigaciones reservadas y que, en ocasiones, interviene en los procedimientos judiciales". Estas investigaciones se basan en "averiguaciones sobre personas y bienes, con la finalidad de garantizar la seguridad de las personas, proteger su patrimonio y velar por el normal desarrollo de sus actividades"[176].

El uso de detectives en el marco de las RRLL sigue aumentado de manera exponencial año tras año[177]. En este sentido, las últimas estadísticas recogidas sobre personal de seguridad privada muestran que, a 31 de diciembre de 2017, constaban como profesionales habilitados 4402 detectives privados en toda España, lo que supone un aumento del 7,68% respecto del año anterior[178].

Cabe destacar que este aumento discurre de forma paralela al crecimiento que el absentismo laboral y las llamadas "bajas fraudulentas" (entendiéndose estas como enfermedades que el trabajador finge con el fin de cobrar la correspondiente prestación) tienen año tras año en nuestro país[179]. En efecto, entre los motivos más frecuentes que dan lugar a la contratación de investigadores privados en el campo que nos ocupa, se encuentra la verificación del estado de salud del trabajador en situación de incapacidad laboral, amén de otras causas como: el seguimiento de empleados que realizan su trabajo a distancia, la comprobación de la existencia de concurrencia desleal, el control sobre el uso del crédito horario del que disfrutan los representantes de los trabajadores, etc[180]. En

---

[175] En este sentido, la STS de 6 de noviembre de 1990 (núm. rec. 93/1990) se pronuncia sobre los detectives privados exponiendo que su uso resulta habitual y en ocasiones, es un "instrumento dotado de exclusividad para el eficaz control por el empresario del exacto cumplimiento de los deberes exigibles al trabajador".

[176] Artículo 2 de la Ley de Seguridad Privada.

[177] DÍAZ RODRÍGUEZ afirma que la contratación de profesionales de la investigación privada en el ámbito laboral ha aumentado de manera considerable desde 2008, en *Detectives y vigilantes privados en el ámbito laboral. Poder empresarial y prueba judicial*, Tirant lo Blanch, Valencia, 2013, pág. 61. Véase también ARIAS DOMÍNGUEZ, A.; SEMPERE NAVARRO, A. V., *Detectives en las relaciones laborales… Op. Cit.,* pág. 59.

[178] Véase la tabla 3-7-4 del en el "Anuario y Estadísticas. Habilitaciones de personal de Seguridad Privada" elaborada por el Ministerio del Interior del Gobierno de España. Disponible en: http://www.interior.gob.es/ca/web/archivos-y-documentacion/seguridad-privada4 (Ultima visita: 24/05/2019).

[179] Véase el VII Informe Adecco sobre Absentismo elaborado por The Adecco Group, págs.: 29 – 31. Disponible en: https://www.adeccogroup.es/wp-content/uploads/2018/06/VII-Informe-Adecco-sobre-Absentismo-Laboral.pdf (última visita: 24/05/2019).

[180] RODRÍGUEZ ESCANCIANO establece como uno de los motivos que originan la investigación hacia un trabajador la necesidad del empresario de verificar la veracidad del estado de salud del empleado, con el fin de constatar que, efectivamente, no es apto para desarrollar la prestación laboral, en *Poder de Control Empresarial… Op. Cit.,* pág. 197. En el mismo sentido se pronuncia DÍAZ RODRÍGUEZ, J. M., *Detectives y*

definitiva, las empresas buscan en la figura del detective un experto capaz de ofrecer elementos de prueba que sirvan para acreditar la existencia o no de incumplimientos laborales en posibles procesos disciplinarios[181].

En cuanto al régimen jurídico de los detectives privados, la prestación de servicios de investigación privada encuentra su fundamento en la Ley de Seguridad Privada (en adelante, LSP) y su reglamento de desarrollo (en adelante, RSP)[182]. Ambas son normas de carácter extralaboral cuyo fin es normalizar tanto la actividad investigadora de los despachos de detectives, como la función de vigilancia y prevención de las empresas de seguridad[183].

Según la LSP, los detectives privados deben contar con la habilitación que emite el Ministerio del Interior y estar inscritos en el Registro Nacional (o autonómico, en su caso) de Seguridad Privada para poder ejercer dicha profesión[184]. Para contratar los servicios de un detective, es necesario que el contratante cuente con un interés legítimo que fundamente el empleo de la investigación privada, como es la protección del rédito empresarial[185]. No obstante, este interés no valida cualquier control, quedando prohibido indagar en la vida íntima de los trabajadores, así como utilizar medios que atenten contra los DDFF de los investigados. Dicha contratación debe formalizarse por escrito y ser puesta en conocimiento del Ministerio del Interior o el órgano autonómico competente en esta materia. Con la firma del contrato, el detective quedará sujeto a un deber de reserva respecto de los datos que conozca con ocasión de su labor investigadora, en virtud del cual solo podrá comunicar los datos o información hallada al contratante y/o "a los órganos judiciales y policiales competentes para el ejercicio de sus funciones". Asimismo, la LSP establece que las actuaciones del detective deben ser razonables,

vigilantes privados… Op. Cit., págs. 58 y 59. Véase también la STS de 15 de octubre de 2014 (núm. rec. 1654/2013).

[181] En relación con la contratación de detectives privados, ARIAS DOMÍNGUEZ y SEMPERE NAVARRO manifiestan que "el empresario busca un trabajo más experto, más cómodo, más rápido y eficaz, y seguramente más profesional, en el sentido de que lo descubierto va a quedar reflejado con mayor propiedad en un informe, que, a su vez, puede servir para sustentar la prueba de lo que se quiere averiguar", en *Detectives en las Relaciones Laborales… Op. Cit.,* pág. 12.

[182] Ley 5/2014, de 4 de abril, de Seguridad Privada y Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.

[183] Véase en este sentido el preámbulo de la LSP.

[184] Artículos 11 y 27 LSP.

[185]Véase DÍAZ RODRÍGUEZ, J. M., *Detectives y vigilantes privados… Op. Cit.,* pág.74. Véase también APARICIO ALDANA, R. K., *Derecho a la intimidad y… Op. Cit.,* pág. 178, donde se expresa que "dado que la conducta del trabajador puede constituir un fraude a la Seguridad Social, tanto esta, como la Mutua de accidentes de trabajo y enfermedades profesionales, se encuentran también legitimadas para realizar las investigaciones".

necesarias, idóneas y proporcionales, por lo que el empleo del detective como herramienta de control empresarial deberá ajustarse al principio de proporcionalidad[186].

Los detectives pueden ejercer la vigilancia de los trabajadores de diferentes formas: bien realizando un seguimiento del investigado donde a través de sus sentidos captan y recogen la información que consideran relevante; o bien, valiéndose de herramientas tales como cámaras de video, fotográficas y/o mediante dispositivos que permitan la grabación de audio. Sin embargo, según la LSP, no cabría definir esta actividad como videovigilancia en sentido estricto, pues considera que dicho tipo de control es el que se hace a través de sistemas de grabación remotos donde la persona que graba no se encuentra presente en el momento en que se registran las imágenes y/o sonidos[187].

La normativa en materia de seguridad privada también contempla la prohibición de contratar los servicios de un detective con el objeto de investigar delitos que puedan ser perseguidos de oficio[188]. Sin embargo, en la práctica este precepto no resulta un impedimento, pues -como ya se ha comentado- las "bajas fingidas" uno de los motivos más habituales por los que empresarios acuden a los servicios de estos profesionales[189].

Durante la actividad investigadora, los detectives pueden obtener información sobre hechos y conductas que afecten a la vida privada del investigado, como por ejemplo, las pruebas relacionadas con su vida laboral, personal, familiar o social. No obstante, no podrán ser objeto de control las conductas que se desarrollen en domicilios particulares sin consentimiento expreso del propietario[190]. Así, por ejemplo, se han declarado nulas por vulneración del derecho a la intimidad del trabajador, las fotografías que un detective

---

[186] Artículos 8, 9, 25, 48, 50 y disposición adicional 2ª LSP.

[187] El artículo 42.1 LSP establece que "los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas". Asimismo, BLÁZQUEZ AGUDO expone que las imágenes y/o audios captados por el detective son un complemento a lo que este percibe, por lo que las grabaciones habitualmente operan "de forma accesoria a la prueba testifical o declaración de la persona que grabó", en *Aplicación práctica de la… Op. Cit.,* pág. 181. En este sentido, véase también la STSJ Canarias 232/2017, de 27 de marzo.

[188] Artículos 101.1.a), 101.2 y 102.1 del RSP y 37 LSP.

[189] Véase en este sentido la noticia "Las bajas fraudulentas ya copan el 90% del trabajo de los detectives privados" del periódico digital El País. Disponible en: https://cincodias.elpais.com/cincodias/2018/10/09/fortunas/1539108545_471618.html (última visita 28/05/2019). Véanse las STS 528/2017, de 20 de junio; y STSJ Madrid 915/2010, de 5 de noviembre.

[190] La CE reconoce la inviolabilidad del domicilio de todo ciudadano en el artículo 18.2. Sobre este aspecto también se pronuncia la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos, que en su artículo 6.5 establece que "no se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial (…) cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia".

realizó desde la calle, donde se mostraba a un trabajador que desempeñando actividades incompatibles con su dolencia mientras se encontraba en el jardín de su domicilio. Sin embargo, el testimonio del detective sí fue permitido, pues la conducta del investigado podía ser observada desde una zona pública por cualquier transeúnte[191].

Para finalizar con su labor de vigilancia, el investigador deberá elaborar un informe con los resultados de la investigación que, junto con el contrato de servicios, servirá como elemento probatorio en posibles procesos disciplinarios[192]. Dicho informe, debe contener todos los datos relativos a la investigación contratada, de modo que, si a través de su labor investigadora el detective descubre irregularidades cometidas por un trabajador distinto, no deberá reflejar este hecho[193].

En cuanto a la necesidad de sospechas previas que justifiquen la adopción de medidas de control ocultas, la doctrina se ha venido pronunciando de manera desigual en este sentido. La jurisprudencia, por su parte, ha resuelto en muchas ocasiones que tales suposiciones justifican la intromisión en la vida privada del trabajador. No obstante, en la medida en que la actividad investigadora debe respetar los DDFF de los ciudadanos, los servicios del detective quedan afectados por el derecho a la protección de datos personales, por lo que se deduce que deberán cumplir con las exigencias del RGPD[194].

De este modo, el empresario debe informar de forma previa, expresa, clara e inequívoca sobre la medida que va a aplicar y su finalidad, no pudiendo atribuir un fin distinto del informado. Asimismo, no cabe el consentimiento del trabajador en este sentido, pues se presume la existencia de una "autorización tácita" entre las partes de una relación laboral,

En este punto, surge una importante cuestión en relación con la obligación de informar del empresario: ¿es la tutela informativa de los trabajadores aplicable a la

[191] Véase la STC 283/2000, de 27 de noviembre.

[192] La mayoría de la doctrina considera que las imágenes y sonidos captados por un detective privado en el curso de su investigación, no resultan una prueba documental independiente del informe, sino que debe valorarse de forma conjunta tanto las grabaciones y/o fotografías, como la intervención del detective y el informe que este elabore. Por tanto, dicha captación de datos del trabajador constituye una prueba testifical. Véase GALIANA MORENO, J. M .; LUJÁN ALCARAZ, J ., "El proceso ordinario y otras modalidades procesales" en *Curso de procedimiento laboral* (MONTOYA MELGAR, A.; GALIANA MORENO, J. M.; SEMPERE NAVARRO, A. V.; RÍOS SALMERÓN, B.; CAVAS MARTÍNEZ, F.; LUJÁN ALCARAZ, J.), Tecnos, 2016, pág. 180. Véase también la STS de 6 de noviembre de 1990 (núm. rec. 93/1990).

[193] Según el artículo 49 LSP, el informe contendrá los datos del contratante, la finalidad del encargo, los detectives que han intervenido, los resultados de la investigación, etc.

[194] Según GONZÁLEZ GONZÁLEZ, C., las grabaciones registradas por detectives privados en el ámbito laboral deben someterse a similares condiciones que las ya expuestas en materia de captación de audio y videovigilancia, en "Control empresarial de la actividad…", *Op. Cit.*, pág. 41.

vigilancia audiovisual que un detective privado puede ejercitar a través de medios informáticos?

En respuesta a esto, numerosos autores se manifiestan de manera contradictoria. Así, por un lado, existe una corriente que justifica el uso de medios subrepticios de control amparándose en distintos motivos como son: la concurrencia de un interés legítimo por parte del empresario[195]; la existencia de fundadas sospechas previas[196]; y la distinción entre el uso de herramientas de control fijas y las móviles y temporales[197]. Por contra, la tendencia opuesta argumenta que: en la medida en que un detective privado puede captar datos personales de un trabajador, este actuará como responsable del tratamiento de dichos datos y deberá de respetar la autotutela informativa tal y como fija el RGPD y el TEDH[198].

En el caso de la videovigilancia, la citada sentencia del Juzgado de lo Social núm. 3 de Pamplona, de 18 de febrero de 2019, ofrecía una solución que bien podría aplicarse al empleo de detectives como medio de control empresarial, esto es, acudir al auxilio judicial para interponer una denuncia solicitando el seguimiento del empleado con cámaras de grabación. De igual forma, el mismo magistrado también ofrece otras soluciones para "salvar" de alguna manera la tutela informativa del trabajador sin dejar de ajustarse a derecho.

En este sentido, el RGPD diferencia dos situaciones con respecto del momento en que ha de practicarse el deber de información: por una lado, si el responsable de tratamiento obtiene los datos directamente del trabajador, la información sobre la finalidad debe ser previa; por otro lado, si el responsable obtiene los datos de manera indirecta como ocurre en el caso del empleo de detectives, este debe informar al trabajador sobre la finalidad de las grabaciones dentro de un plazo razonable que, tal y como especifica la normativa, será en el momento en que el investigador entregue las grabaciones al empresario que solicitó sus servicios y, en todo caso, antes de un mes desde la grabación[199].

---

[195] DÍAZ RODRÍGUEZ, J. M., *Detectives y vigilantes privados… Op. Cit.,* pág.76. En el mismo sentido, se pronuncia la AEPD indicando que las grabaciones realizadas por detectives privados con base en un contrato debidamente motivado no quedan sometidas al consentimiento ni al deber informativo, según las resoluciones de 2 de octubre de 2008 y la núm.1396/2013.

[196] DESDENTADO BONETE, A., y MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y… Op. Cit.,* pág. 29.

[197] DOCTOR SÁNCHEZ-MIGALLÓN, R., "La vigilancia de la actividad del trabajador mediante videocámaras y circuitos cerrados de televisión", *IUSLabor*, núm. 3, 2014, pág. 10.

[198] Ejemplo de esta corriente es GONZÁLEZ GONZÁLEZ, C., "Control empresarial de la actividad…", *Op. Cit.*, pág. 43.

[199] Artículos 13 y 14 RGPD.

Esta diferenciación en la forma de obtener los datos personales parece hacer referencia a los distintos ámbitos espaciales y horarios donde el empresario puede ejercer su control. Es decir, si la vigilancia se lleva a cabo en el lugar de trabajo y dentro de la jornada laboral, el empresario será el responsable de tratamiento y los datos del trabajador serán entregados por él mismo. Sin embargo, en el supuesto de vigilancia practicada fuera del ámbito empresarial, el responsable del tratamiento será el detective y obtendrá los datos de manera indirecta a través de grabaciones y/o fotografías[200].

Asimismo, el artículo 22 LOPDGDD establece que el tratamiento por parte el empleador de los datos personales con fines de videovigilancia habrá de atenerse a lo dictado en el artículo 89 de la misma ley que, a su vez, viene a referirse al control de la prestación dentro del lugar de trabajo[201]. Esto parece indicar que la vigilancia ejercitada más allá del espacio empresarial quedaría regulada por la LSP[202]. Sin embargo, a pesar de que la normativa de seguridad privada fija el principio de reserva según el cual el trabajador no tendría derecho a acceder a sus propios datos, este precepto no entraría en juego en situaciones de control audiovisual practicadas por un detective privado[203]. Pues, ya que el RGPD prima sobre normativas de rango inferior en los preceptos que se encuentren en contra, una vez más tropezaríamos con el derecho a la tutela informativa de los trabajadores.

A mi juicio, un sistema de control audiovisual fijo y permanente resulta claramente más invasivo para los DDFF de los trabajadores que la vigilancia que se ejerce de manera ocasional, pues permite vigilar la conducta del empleado en todo momento. De este modo, ante fundadas sospechas sobre la existencia de ilícitos laborales por parte de un trabajador, puede adecuado que la investigación privada sea una de las excepciones al cumplimiento del deber de informar. De lo contrario, empleados sospechosos de irregularidades laborales podrían seguir actuando fraudulentamente sin consecuencia alguna amparándose en la nulidad de las actuaciones causada por la falta del deber de información empresarial.

[200] GONZÁLEZ GONZÁLEZ, C., "Control empresarial de la actividad…", *Op. Cit.*, pág. 46

[201] Concretamente, el artículo 89 LOPDGDD se denomina "Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo".

[202] El artículo 22.7 LOPDGDD establece que el tratamiento con fines de videovigilancia se entiende sin perjuicio de lo previsto en la LSP y sus disposiciones de desarrollo.

[203] El artículo 50 LSP fija el deber de reserva que tienen los profesionales de la seguridad privada según el cual los detectives en ejercicio solo podrán facilitar los datos personales a las personas que le encomendaron el servicio o las autoridades.

En definitiva, resulta evidente que, mientras que la relación entre el uso de detectives privados en el ámbito laboral y el derecho a la intimidad de los trabajadores (ya sea dentro o fuera del ámbito espacial de la empresa) parece clara, la regulación de la protección de datos de carácter personal en el marco de la investigación privada de los trabajadores se torna más difusa. En este sentido, podría resultar de gran relevancia una "modernización" de la LSP que dibujara unos límites más claros en relación con el control del trabajador fuera del centro de trabajo o la jornada laboral. Hasta ese momento, no cabe duda de que el control empresarial de la actividad mediante detectives y el derecho de los trabajadores a la protección de datos seguirá suscitando grandes controversias.

2.- LA MONITORIZACIÓN DEL ORDENADOR DE LOS TRABAJADORES

La generalización informática que vive la sociedad actual también se ha extendido al mundo empresarial, trayendo consigo nuevos modos e instrumentos de trabajo basados en las NTIC. Hoy, resulta habitual que los trabajadores cuenten con material informático (como un ordenador, una tableta, o un *smartphone*) del que se sirvan para el desempeño de la actividad laboral. Así, el ordenador y la navegación a través de internet se han convertido en herramientas esenciales para cualquier organización[204].

El uso del ordenador como herramienta de trabajo supone un gran intercambio de información que los trabajadores pueden llevar a cabo a través de canales como la intranet de la empresa, los correos electrónicos, o la navegación en internet. En este sentido, el control empresarial puede resultar conflictivo pues, el acceso a los datos contenidos en el ordenador (u otro soporte de almacenamiento al que se acceda desde la computadora, como por ejemplo, la nube) podría colisionar con los DDFF a la intimidad, al secreto de las comunicaciones y a la protección de datos de los trabajadores.

Con la monitorización del ordenador, las empresas buscan mejorar la calidad de los servicios prestados, comprobar el nivel de *presentismo* de la plantilla y/o vigilar el empleo

[204] La "Encuesta sobre el uso de la TIC y comercio electrónico de las empresas" elaborada por el Instituto Nacional de Estadística (datos referidos al año 2017 y el primer trimestre de 2018), expone que el 79,80% de las empresas españolas con menos de diez empleados dispone de ordenadores, mientras que el 75,54% tienen acceso a internet. En cuanto a las empresas con más de diez trabajadores, el 99,22% cuenta con ordenadores, y el 98,65% dispone de acceso a internet. Disponible en: https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176743&menu=ultiDatos&idp=1254735576799 (última visita: 03/06/2019).

que los trabajadores hacen de las herramientas de trabajo[205]. De este modo, el registro de la navegación en internet y de los correos electrónicos destacan entre los tipos de control a los que el empresario recurre con mayor frecuencia[206].

Si bien es cierto que el ET habilita al empleador a ejercer la vigilancia sobre los trabajadores con el fin de verificar el efectivo cumplimiento de la prestación laboral, no todo control es válido[207]. Por lo que el empresario solo podrá monitorizar el ordenador del que sea titular, en caso contrario, la empresa lesionará el derecho a la propiedad privada del trabajador[208]. Asimismo, si el control empresarial es ilegítimo, el resultado que se derive del mismo también lo será, no pudiendo aportarse como elemento de prueba en un proceso judicial[209].

En este orden de ideas, la cuestión principal gira en torno a dos aspectos: por un lado, el uso -laboral o personal- que el trabajador hace del ordenador puesto a su disposición por la empresa; y, por otro, los límites que determinan la legitimidad del control empresarial sobre las herramientas informáticas. Pues bien, debido a la falta de normativa específica que existía en relación con esta materia, han sido los tribunales los encargados de sentar las bases en este sentido[210].

A este respecto se ha pronunciado el TS manifestando que, el empleador, en virtud del artículo 20.3 ET, puede realizar registros informáticos a cualquier hora y lugar, no siendo imprescindible la presencia del trabajador[211]. Asimismo, resulta necesario que el

---

[205] El presentismo puede definirse como "el comportamiento consistente en acudir al puesto de trabajo dedicando el tiempo a otros quehaceres no relacionados con el propio puesto de trabajo ni con la empresa", según el VII Informe Adecco sobre Absentismo, elaborado por The Adecco Group, pág. 13. Disponible en: https://www.adeccogroup.es/wp-content/uploads/2018/06/VII-Informe-Adecco-sobre-Absentismo-Laboral.pdf (última visita: 05/06/2019).

[206] BLÁZQUEZ AGUDO, E. M., *Aplicación práctica de la…Op. Cit.*, pág. 169. En este sentido, véanse los Informes Jurídicos de la AEPD núm. 0391/2017 y núm. 0242/2008, sobre el control del trabajador a partir del filtrado de correos electrónicos. Disponible en: https://www.aepd.es/informes/historicos/2008-0242.pdf (última visita: 04/06/2019).

[207] El artículo 20.3 ET establece que "el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales". Véase también el artículo 87 LOPDGDD.

[208] Véase el artículo 33 CE.

[209] En este sentido, SAN MARTÍN MAZZUCCONI y SEMPERE NAVARRO afirman que "las pruebas obtenidas sin haber advertido previamente al trabajador sobre la fiscalización del uso del ordenador carecen de validez", en, *Las TICs en… Op. Cit.*, pág. 14. Véase también la ponencia de CAVAS MARTÍNEZ, "Los Derechos y Libertades Fundamentales en materia laboral", realizada en el marco del I Seminario del Área de Derecho del Trabajo y la Seguridad Social, el 23 de febrero de 2015 en la Universidad Miguel Hernández de Elche (Alicante). Disponible en: https://www.youtube.com/watch?v=fECK5u0FO6A (última visita: 05/06/2019).

[210] Téngase en cuenta que tanto el RGPD como la LOPDGDD entraron en vigor en mayo y diciembre del año 2018, respectivamente.

[211] Tal y como afirma la STS de 8 de marzo de 2011 (núm. rec. 1826/2010), si el ordenador es propiedad de la empresa, no será de aplicación el artículo 18 ET según el cual, el trabajador (o, en su defecto, un

empresario informe a los trabajadores sobre el uso que deben hacer de los instrumentos de trabajo, de forma previa y con la debida claridad. De este modo, si la empresa prohíbe el uso personal de la computadora habrá eliminado la "razonable expectativa de confidencialidad" que pudiera tener el trabajador y, por consiguiente, se permite la fiscalización del ordenador, quedando minimizada la posible lesión de los DDFF de los trabajadores[212]. Esta expectativa de privacidad hace referencia a la creencia del empleado de que, dentro de su jornada laboral, existe un espacio reservado donde puede actuar de manera libre sin que el empresario pueda tener acceso[213].

No obstante, si bien la expectativa de confidencialidad pueda ser neutralizada con la existencia de códigos de conducta sobre el uso de las NTIC en la empresa, el TC dicta que la medida empresarial de monitorización debe superar el principio de proporcionalidad. Por lo que el control del ordenador debe estar justificado, ser necesario (que no exista otra medida menos invasiva para los DDFF de los trabajadores que cumpla con la finalidad que busca el empresario), idóneo (la medida debe ser capaz de cumplir con la finalidad que busca el empresario) y proporcional en sentido estricto (de la medida empresarial deben derivar más ventajas que inconvenientes)[214].

En caso de no existir una política empresarial de uso de las herramientas informáticas, la jurisprudencia ha venido aceptando la presencia de una "autorización tácita" entre los miembros de la relación contractual que aprueba el eventual uso personal de los dispositivos tecnológicos. Esta autorización solo podrá verse contravenida a través de una prohibición expresa y establecida, ya sea por la normativa o convenio colectivo aplicable, o bien, mediante una orden empresarial[215].

Siguiendo esta doctrina, posteriores resoluciones han admitido la validez de las prohibiciones absolutas del uso personal del ordenador, así como la presunción de

---

compañero o un representante de los trabajadores) debe estar presente durante los registros que pudieran realizarse sobre su taquilla o efectos personales.

[212] BLÁZQUEZ AGUDO, E. M., *Aplicación práctica de la… Op. Cit.*, pág. 171. Véase la STC 241/2012, de 17 de diciembre, que declara que no existe lesión del derecho a la intimidad ni del secreto de las comunicaciones de una trabajadora que instaló un programa de mensajería instantánea en el ordenador de la empresa para usos particulares. Véanse también las SSTS de 8 de marzo de 2011 (núm. rec. 1826/2010); y de 26 de septiembre de 2007 (núm. rec. 966/2006).

[213] Véase la definición que ofrece el "Diccionario del español jurídico" de la Real Academia Española sobre el término "expectativa de privacidad". Disponible en: https://dej.rae.es/lema/expectativa-de-privacidad (última visita: 10/06/2019).

[214] SAN MARTÍN MAZZUCCONI, C.; SEMPERE NAVARRO, A. V., *Las TICs en el… Op. Cit.*, pág. 15. Véanse también las SSTC 96/2012, de 7 de mayo; 37/1998, de 17 de febrero, FJ 8º; 207/1996, de 16 de diciembre, FJ 4º; 55/1996, de 28 de marzo, FJ 6º – 9º; y 66/1995, de 8 de mayo, FJ 5º.

[215] Véase la STC 170/2013, de 7 de octubre, en la que el convenio colectivo aplicable contenía un precepto sobre el uso exclusivamente profesional del correo electrónico propiedad de la empresa, constituyendo como infracción grave el uso para diferentes fines.

prohibición del uso particular en caso de que dicha conducta se tipifique como sanción en el Convenio Colectivo aplicable[216]. En el mismo sentido, ulteriores sentencias han interpretado esta doctrina inadmitiendo las medidas de control empresarial cuando no existía una política previa sobre el uso de los ordenadores[217].

Así, a pesar de la existencia de una corriente jurisprudencial más restrictiva que permite las prohibiciones absolutas del uso privado de los dispositivos tecnológicos, la tendencia actual se caracteriza por ser más flexible, tolerando un uso personal moderado del ordenador[218]. De este modo, para valorar si el uso que un empleado da al ordenador es moderado no abusivo, los tribunales han dictado la necesidad de examinar si hay un perjuicio derivado de un uso indebido y cuál es su intensidad[219].

Sobre este extremo se ha pronunciado el TEDH en su sentencia de 5 de septiembre de 2017 en el asunto *Bârbulescu* v. Rumanía (también conocida como *Bârbulescu* II) confirmando que, en efecto, todo empleado goza de una expectativa razonable de privacidad en el trabajo.

La STEDH aborda el supuesto en el que una empresa, que contaba con una política de uso de los medios de comunicación y tecnológicos donde se prohibía su uso personal, despide a un trabajador por utilizar un servicio de mensajería instantánea para fines particulares. Concretamente, el empleado -ingeniero comercial- había creado la cuenta de mensajería para mantener el contacto con los clientes por petición de la empresa. La empresa, que había puesto en conocimiento del trabajador el código de conducta empresarial en el momento de la firma del contrato de trabajo, monitorizó las conversaciones descubriendo que el ingeniero mantenía contacto con familiares y amigos de manera habitual. Ante estos hechos, la empresa comunicó el despido a su empleado

[216] Véanse la STS de 6 de octubre de 2011 (núm. rec. 4053/2010) que admitió la prohibición absoluta del uso particular; y la STC 170/2013, de 7 de octubre, que trae causa el despido disciplinario de una trabajadora cuya empresa, ante sospechas de incumplimientos laborales, entrega el ordenador (propiedad de la empresa) a un Notario.

[217] Así lo han interpretado las SSTSJ Madrid 453/2011, de 30 de mayo; Madrid, 346/2011, de 28 de abril; y Cantabria 546/2009, de 24 de junio; entre otras.

[218] DESDENTADO BONETE se manifiesta sobre estas dos corrientes (estricta y flexible) en su ponencia "Nuevas tecnologías y las relaciones laborales" presentada en el *XIII Foro Aranzadi Social 2012-2013*, en Madrid, el 10 de abril de 2013. Véase también SAN MARTÍN MAZZUCCONI, C.; SEMPERE NAVARRO, A. V., *Las TICs en el… Op. Cit.*, págs. 11 y 12.

[219] Véanse las SSTSJ Cantabria de 13 de noviembre de 2012 (EDJ 130230); Cataluña, de 15 de octubre de 2003 (núm. rec. 3637/2003); Castilla y León 512/2004, de 29 de marzo; y Galicia 4168/2001, de 4 de octubre; que examinan el perjuicio que un uso indebido de las herramientas informáticas de trabajo puede tener sobre la empresa, para valorar si la existencia de una transgresión de la buena fe contractual por parte del trabajador. En este sentido véase la STSJ Cataluña 1506/2003, de 5 de marzo, que valora la intensidad del uso indebido analizando la duración del tiempo que el trabajador pasaba en páginas web no relacionadas con su prestación laboral.

quien, en primer lugar negó la existencia de tales conversaciones. Por ello, la empresa accedió al contenido de las comunicaciones privadas para transcribirlas e imprimirlas, informando de este aspecto al trabajador. El empleado impugnó el despido por entender que sus derechos a la intimidad y al secreto de las comunicaciones habían sido lesionados.

Así, el pleito alcanzó al TEDH, quien resolvió que la empresa había vulnerado el artículo 8 CEDH, declarando la nulidad del despido. La STEDH de 5 de septiembre de 2017, destaca por indicar qué elementos son los que deben ponderarse para valorar la legitimidad del control empresarial sobre las herramientas informáticas de los trabajadores, sentando así una importante doctrina en relación con el uso del ordenador y las comunicaciones electrónicas en el ámbito laboral.

En este sentido, el TEDH establece que toda medida empresarial debe superar una serie de requisitos para valorar si es ajustada a derecho, comprendidos en el llamado "test *Bârbulescu*", esto es: primero, el empresario debe informar -de manera previa y clara- al trabajador que sus comunicaciones pueden ser intervenidas; segundo, habrá que analizar el grado de intrusión del empresario en las comunicaciones del trabajador atendiendo al tiempo durante el cual se ha monitorizado el ordenador (quedando el control limitado al estrictamente necesario para constatar el cumplimiento de las obligaciones laborales de los trabajadores), al número de personas que han tenido acceso al contenido de las comunicaciones y si ese acceso ha sido en todo o parte; tercero, el empresario debe contar con una motivación legítima para fiscalizar las herramientas de trabajo que puede ser fundamentada en la existencia de sospechas previas; cuarto, no deben existir métodos de control menos invasivos para los trabajadores que permitan al empresario conocer el cumplimiento de los deberes de sus empleados; quinto, la empresa debe utilizar el resultado de la monitorización para el fin perseguido (verificar el correcto desarrollo de la prestación laboral); sexto, deben existir mecanismos que permitan informar al trabajador en caso de que el empresario acceda a sus conversaciones.

Esta serie de criterios son de carácter acumulativo, esto es, el incumplimiento de cualquiera de ellos supondrá la nulidad de la medida de control empresarial por vulneración de los DDFF de los trabajadores. Y, en consecuencia, las pruebas que se hayan podido obtener con ocasión de la monitorización ilegítima serán nulas[220].

[220] Véase en este sentido la sentencia del Juzgado de lo Social núm. 17 de Madrid, de 17 de noviembre de 2017, que aplica la doctrina de la STEDH *Bârbulescu* II, declarando nulo el despido fundamentado en la monitorización de las comunicaciones electrónicas que no fueron admitidas en el proceso por vulnerar los DDFF a la intimidad y al secreto de las comunicaciones de un trabajador.

No obstante la importancia de esta sentencia, recientes pronunciamientos concluyen que los citados requisitos fijados por el TEDH se integran en el test de proporcionalidad que ya venía siendo exigido por nuestro ordenamiento jurídico, por lo que no se deriva ninguna consecuencia relevante de la instauración de esta doctrina en el sistema legal español[221].

Con respecto a la normativa específica en relación con el control informático del trabajador, el artículo 87 de la reciente LOPDGDD, resulta continuador de la doctrina que tanto el TEDH como los tribunales españoles han venido aplicando. Así, el precepto sobre el "derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral", dispone lo siguiente: "1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador; 2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos; 3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores. El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado".

En resumen, podemos afirmar que, tanto la doctrina como la jurisprudencia manifiestan que las medidas de control empresarial deben ser valoradas en atención al uso que los empleados les dan y a las órdenes que el empresario haya dispuesto[222], pues no existen reglas universales y habrá que atender a las circunstancias particulares en cada supuesto, si bien el control debe ser proporcional, en todo caso[223]. Asimismo, la existencia

[221] A modo de ejemplo, véase la STS 119/2018, de 8 de febrero, que analiza (por primera vez en España) el cumplimiento por parte de una empresa de la doctrina fijada por la STEDH *Bârculescu* II, en relación con el control empresarial de los correos electrónicos de los trabajadores; y la sentencia del Juzgado de lo Social núm. 17 de Madrid, de 17 de noviembre de 2017.
[222] Así lo afirma el TC en su sentencia 241/2012, de 17 de diciembre.
[223] ROQUETA BUJ, R., "El derecho a la intimidad…", *Op. Cit.*, págs. 444 – 446.

de una política de empresa clara y actualizada sobre uso del ordenador, así como la puesta a disposición del trabajador de un manual de buenas prácticas, resulta clave en este sentido, pues la ausencia de limitaciones expresas siempre jugará a favor del trabajador, tal y como hemos visto[224]. En definitiva, el control de las herramientas informáticas resulta una materia de gran dinamismo, donde no pueden descartarse futuros cambios de criterio por parte de los tribunales[225].

3.- LA GEOLOCALIZACIÓN DE LOS TRABAJADORES

Los sistemas de geolocalización, también conocidos por sus siglas en inglés como GPS (*global positioning system)*, son herramientas que permiten conocer la ubicación de un dispositivo en tiempo real y en un punto geográfico determinado. Su utilización como herramienta de navegación ha posibilitado la extensión de su uso entre la sociedad, destacando su aplicación tanto a vehículos como a teléfonos inteligentes. Esta generalización, se ha visto reflejada en el mundo laboral, cuya implantación es relativamente reciente[226].

El uso del GPS como instrumento de control empresarial encuentra su fundamento en el artículo 20.3 ET y faculta al empleador a realizar un seguimiento más o menos exhaustivo de los desplazamientos de un trabajador. Esta forma de vigilancia puede ser muy útil en ciertos tipos de prestación laboral tales como el transporte de mercancías, pues facilita la organización del trabajo y el control de un vehículo en todo momento[227]. Sin embargo, puede resultar un medio de control muy invasivo, pues el acceso del

[224] SAN MARTÍN MAZZUCCONI, C.; SEMPERE NAVARRO, A. V., *Las TICs en el… Op., Cit.,* pág. 23. Véase la recomendación CM/Rec(2015)5, del Consejo de Ministros de la Unión Europea. Disponible en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a (última visita: 01/07/2019). Véanse también las SSTSJ País Vasco de 21 de diciembre de 2004 (EDJ 254091); Cantabria de 1 de marzo de 2004 (EDJ 40113); Madrid, 22 de noviembre de 2002 (núm. rec. 3806/02).
[225] Tanto la STS, de 6 de octubre de 2011, como la STC 241/2012, de 17 de diciembre, son muestra de la complejidad de la materia, pues ambas cuentan con votos particulares que reflejan las distintas opiniones en relación con esta temática.
[226] RODRÍGUEZ ESCANCIANO, S., *Poder de Control Empresarial… Op. Cit.,* pág. 105.
[227] LLAMOSAS TRAPAGA, A., *Relaciones laborales y nuevas… Op. Cit.*, pág. 164.

empresario a tal cantidad de datos puede generar una intromisión ilegítima en los DDFF de los trabajadores[228].

Los sistemas GPS permiten la creación de ficheros de datos de geolocalización que, según la AEPD, son datos de naturaleza personal puesto ya que "siempre se refieren a una persona física identificada o identificable"[229]. Así, la medida de control empresarial basada en la geolocalización de los trabajadores deberá someterse a las determinadas exigencias previstas en materia de protección de datos, entre las que destaca el deber informativo del empresario. Es decir, el empresario debe informar previamente y de forma expresa, clara e inequívoca a los trabajadores (y/o a sus representantes legales) sobre la instalación del GPS, su finalidad y la posibilidad de ejercer sus derechos ARCO[230].

No cabe, por tanto, anunciar una finalidad distinta de la real o, realizar un uso distinto del informado. Ejemplo de ello es la STSJ Madrid de 21 de marzo de 2014 que declara ilícita la medida empresarial basada en la instalación de un GPS en el vehículo puesto a disposición del trabajador por vulnerar el derecho a la protección de datos del empleado en su vertiente informativa, puesto que la empresa había afirmado que la finalidad del GPS era la seguridad de sus empleados.

Asimismo, no es necesario que el trabajador autorice la instalación del dispositivo GPS, si bien, el deber informativo deberá cumplirse en todo caso[231]. Esta falta de consentimiento encuentra su fundamento en el uso laboral que el trabajador hace de la herramienta puesta a disposición por el empresario[232]. Por tanto, si la empresa autoriza el

---

[228] En este sentido, la STSJ Madrid de 21 de marzo de 2014 afirma en su FJ 4º que el GPS permite mantener "el permanente conocimiento de parcelas de la vida del trabajador que por muy imbricadas que estén en el desarrollo de la relación laboral con la empresa inciden potencialmente en la esfera de su derecho a la intimidad personal y, de ser objeto de tratamiento como aquí sucede, del que igualmente le asiste a la protección de datos de tal carácter". Véase también la entrada "Control empresarial y Geolocalización" realizada por PURCALLA BONILLA en el blog del profesor FERNÁNDEZ GARCÍA, https://aflabor.wordpress.com/. Disponible en: https://aflabor.wordpress.com/2017/07/21/control-empresarial-y-geolocalizacion-colaboracion-de-miquel-angel-purcalla-bonilla/ (última visita: 13/06/2019).

[229] Véase el Informe Jurídico núm. 0090/2009 de la AEPD sobre la proporcionalidad en el tratamiento de los datos de localización. Disponible en: https://www.aepd.es/informes/historicos/2009-0090.pdf (última visita: 14/06/2019).

[230] Véase el artículo 90.2 LOPDGDD, sobre el "Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral". Véase también el apartado 2.2 sobre "La prueba en el procedimiento laboral" del presente trabajo donde se explica más detalladamente qué derechos comprenden los denominados como ARCO.

[231] El deber de información venía siendo una exigencia de los tribunales en relación con el deber de buena fe contractual que el empresario debe al trabajador, ejemplo de ello es la STSJ País Vasco de 2 de junio de 2007.

[232] El TC establece que el contrato de trabajo implica "un consentimiento implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes" en su sentencia 39/2016, de 3 de marzo (FJ 3º).

uso personal de un coche o teléfono móvil no cabrá el control de la localización del trabajador fuera de su jornada laboral, salvo la autorización expresa de este último[233].

Del mismo modo, si la herramienta sobre la que se implanta el GPS es propiedad del empleado será obligatorio el consentimiento del titular del bien objeto de vigilancia. En este sentido, se ha pronunciado el TS declarando que la instalación de un GPS en el coche particular del trabajador vulnera tanto el derecho a la propiedad privada como el derecho a la intimidad de este último, siendo necesaria la autorización expresa del empleado en todo caso[234].

En adición al deber informativo y al consentimiento del trabajador (en las situaciones que así lo exijan), la jurisprudencia ha venido aplicando el triple examen de proporcionalidad a las medidas de control empresarial basadas en dispositivos GPS[235]. De este modo, las medidas limitadoras de DDFF deberán estar debidamente justificadas en un interés constitucionalmente protegible (como es el interés empresarial amparado en el artículo 35 CE sobre la libertad de empresa), y deben someterse al juicio de idoneidad (la medida de control ha de ser capaz de conseguir el objetivo de vigilancia perseguido por la empresa), necesidad (no debe existir otro medio de control menos invasivo para el trabajador que cumpla con la finalidad que busca el empresario) y proporcionalidad en sentido estricto (de la medida adoptada deberán desprenderse más beneficios para la sociedad que desventajas para los trabajadores) [236].

Esta serie de requisitos son los necesarios para la licitud del uso fiscalizador del GPS, sin embargo, los pronunciamientos en este sentido han seguido criterios desiguales debido a la falta de concreción normativa existente hasta hace bien poco. Así, el deber informativo se volvía más riguroso o flexible según la sala que lo aplicase.

La actual normativa en materia de protección de datos incluye ciertas pautas en el uso de los sistemas de geolocalización en el ámbito laboral que venían siendo recogidas por la jurisprudencia. Así, el artículo 90 LOPDGDD establece los siguiente: "1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización

---

[233] Véanse las SSTSJ Asturias de 16 de noviembre de 2017; Andalucía de 15 de julio de 2015.

[234] Véase la STS de 21 de junio de 2012 que considera desproporcionada la medida de vigilancia consistente en un GPS que un detective privado instala en el coche de un trabajador en situación de incapacidad laboral cuya empresa tiene sospechas de la realización de actividades incompatibles con su estado de salud. Véase también el Informe Jurídico núm. 0193/2008 de la AEPD. Disponible en: https://www.aepd.es/informes/historicos/2008-0193.pdf (última visita: 15/06/2019).

[235] En este sentido véase SAN MARTÍN MAZZUCCONI, C.; SEMPERE NAVARRO, A. V., *Las TICs en el… Op., Cit.*, pág. 65.

[236] Véanse las SSTC 96/2012, de 7 de mayo; 55/1996, de 28 de marzo, FJ 6º – 9º; 207/1996, de 16 de diciembre, FJ 4º; 66/1995, de 8 de mayo, FJ 5º; y 37/1998, de 17 de febrero, FJ 8º.

para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo; 2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión".

Asimismo, el artículo 88 LOPDGDD sobre el Derecho a la desconexión digital en el ámbito laboral establece que "los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar (…) se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas". Este precepto, sin duda, puede vincularse con el derecho de los trabajadores a no estar localizables mientras se encuentren fuera de su jornada laboral.

En este contexto normativo actual, surge una interesante resolución de la Audiencia Nacional (en adelante, AN), de 6 de febrero de 2019, sobre la geolocalización de los trabajadores a partir de dispositivos particulares. En este caso, la cadena de comida rápida Telepizza implanta un sistema de seguimiento de los pedidos en los teléfonos móviles particulares de los trabajadores repartidores. En el contrato de trabajo diversas cláusulas estipulaban la obligatoriedad de los trabajadores de disponer de un teléfono inteligente donde instalar la aplicación que permitiría su geolocalización durante la jornada de trabajo, motivo por el cual la empresa compensaba con 3,50€ mensuales a cada trabajador. Asimismo, el contrato disponía que en caso de incumplir dichos cometidos podría llegar a despedirse al trabajador.

La AN declaró que la medida de control empresarial resultaba desproporcionada argumentando que se podían haber utilizado medidas menos invasivas para la intimidad de los trabajadores como, por ejemplo, un sistema de GPS en las motocicletas de reparto. Asimismo, dictó que las cláusulas contractuales por las que los trabajadores tenían que aportar su propio teléfono y podían ser despedidos eran nulas. Resolvió que la obligación de aportar herramientas de trabajo propiedad del empleado constituía un abuso de derecho

del empresario y que, además, este no cumplió con el deber de consulta a los representantes de los trabajadores que regula el artículo 64.5.f) ET.

Para finalizar, en atención a la problemática que surge con ocasión del uso de dispositivos GPS en el marco de las RRLL, cabe concluir lo siguiente: primero, el control empresarial solo puede realizarse durante la jornada laboral; segundo, la medida debe superar el test de la proporcionalidad (debe ser idónea, necesaria, equilibrada y estar debidamente justificada); tercero, los datos de localización son de carácter personal, por lo que su tratamiento deberá ajustarse a la normativa en este sentido y, por ende, el empresario deberá cumplir con su deber de informar de manera previa, expresa, clara e inequívoca sobre la existencia y finalidad del GPS; cuarto, el empresario deberá cumplir con el derecho de consulta de los representantes de los trabajadores; quinto, el empresario no puede establecer de manera unilateral la obligatoriedad de que sus empleados aporten sus bienes personales como herramientas de trabajo ni imponer un sistema disciplinario que no recoja el ET o el convenio colectivo de aplicación; y sexto, el consentimiento del trabajador deberá exigirse según las circunstancias de cada caso.

4.- EL CONTROL BIOMÉTRICO DE LOS TRABAJADORES

El avance tecnológico y su aplicación a diferentes ámbitos de la sociedad ha propiciado el aumento del uso de técnicas tan novedosas como la biometría. La biometría es la ciencia encargada de estudiar las distinciones morfológicas y del comportamiento humano con el fin de verificar una identidad en particular. Así, la tecnología biométrica se configura como un método de reconocimiento basado en el análisis de las características físicas y conductuales tales como la huella dactilar, la voz, o el iris, que permiten la identificación de un individuo[237].

Centrándonos en el marco de las RRLL, estos nuevos medios se ponen a disposición de los empresarios como una herramienta más de control cuya aplicación más usual es el control horario de los trabajadores[238]. Así, el control biométrico resulta de especial

[237] Véase la Guía "Tecnologías biométricas aplicadas a la ciberseguridad" elaborada por el Instituto Nacional de Seguridad (INCIBE), págs. 4 y 5. Disponible en: https://www.incibe.es/protege-tu-empresa/guias/tecnologias-biometricas-aplicadas-ciberseguridad-guia-aproximacion-el (última visita: 14/06/2019).

[238] En este sentido, BLÁZQUEZ AGUDO afirma que "es muy usual que las empresas hayan sustituido el sistema de control de entrada y salida tradicional de fichaje por otros biométricos, especialmente mediante huella digital", en *Aplicación práctica de la… Op. Cit.*, pág. 202. Véanse las SSTSJ Cantabria, de 10 de enero de 2003 (núm. rec. 517/02) y de 28 de marzo de 2003 (núm. rec.759/02), que establecen que los

relevancia en relación con la reciente ley sobre registro horario, cuyo fin es realizar seguimiento sobre el horario de los trabajadores, concediéndoles, a su vez, un elemento que pruebe la jornada de trabajo efectivamente realizada[239].

Según el Instituto Nacional de Ciberseguridad, los sistemas biométricos permiten una mayor eficacia en el control de accesos, de presencia y en la lucha contra el fraude. Asimismo, la aplicación de estas técnicas ofrece al empresario un aumento de la seguridad en el control de entrada y salida, una mejora de la imagen corporativa, y una mayor la privacidad pues los sistemas biométricos cifran los datos reales de los usuarios[240].

Ahora bien, este nuevo tipo de control también plantea nuevos problemas tales como la licitud de la implantación de lectores de huella dactilar para el control horario de los trabajadores. En este sentido, la AEPD ha venido declarando como válido la instalación de sistemas de control de asistencia basados en la lectura de la huella dactilar de los trabajadores, sin necesidad de recabar el consentimiento de los afectados. Así, el Informe Jurídico núm. 0000/1999 que estudia la validez del dispositivo biométrico de control instalado en una Corporación Local, establece que los datos biométricos son datos personales que no representan ningún aspecto concreto de la personalidad del individuo, por lo que simplemente tratan de identificarlos sin tener sus datos mayor trascendencia que un número de identificación personal[241]. Del mismo modo, el Informe Jurídico núm. 0340/2007 de la AEPD declara que la huella dactilar no contiene información personal alguna, por lo que no resulta un elemento invasivo para el trabajador[242].

El TS, por su parte, ha manifestado que recabar datos biométricos de los trabajadores con el fin de controlar la asistencia al centro de trabajo no lesiona los DDFF a la intimidad y a la protección de datos. El alto Tribunal argumenta que los lectores biométricos no "fotografían" la mano y huellas de los empleados, sino que transforman los datos captados en un algoritmo haciendo irreconocible la mano y/o huella del trabajador a simple vista[243].

---

sistemas de fichaje informático que emplean datos biométricos como la lectura de la mano resultan mecanismos de control mucho más sofisticados que la videovigilancia o la captación de audio.

[239] El artículo 34.9 del Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, estable la obligación legal de registrar la jornada de trabajo de todos los trabajadores de una empresa.

[240] Véase la Guía "Tecnologías biométricas aplicadas a la…", *Op. Cit.*, págs. 13 – 22.

[241] Informe Jurídico núm. 0000/1999 de la AEPD.

[242] Informe Jurídico núm. 0340/2007 de la AEPD.

[243] Véase la STS de 2 de julio de 2007 (núm. rec. 5017/2003) que trae causa la validez de la instalación de un lector biométrico de la mano (y por ende, de la huella dactilar) de los empleados públicos de Cantabria. En este mismo sentido la STSJ Andalucía 874/2007, de 3 de diciembre, expone que "la recogida de los datos biométricos por sistemas informáticos (…) no vulneran su derecho fundamental, puesto que ni

Así las cosas, con la entrada en vigor del RGPD se producirían diversas novedades en relación con los datos biométricos. En primer lugar, el RGPD cataloga los datos biométricos como datos personales de categoría especial, dándoles así una mayor protección respecto de la anterior normativa en materia de protección de datos. Seguidamente, el artículo 9 RGPD prohíbe el tratamiento de datos biométricos, si bien el mismo precepto ofrece diversas excepciones por las que dicha prohibición no será de aplicación cuando: el interesado dé su consentimiento de manera expresa; o el tratamiento resulte necesario para que el responsable cumpla con sus obligaciones y con los derechos de los afectados en el ámbito laboral, si así lo autoriza el Derecho de la UE o un Convenio Colectivo[244]. Además, el tratamiento de datos biométricos deberá respetar los DDFF de los afectados, en todo caso.

En cuanto a la normativa estatal en materia de protección de datos, la LOPDGDD no incluye una regulación específica sobre técnicas o datos biométricos. Por lo que serán aplicables las exigencias ya tenidas en cuenta en anteriores apartados para otros tipos de control que almacenan y/o registran datos personales de los trabajadores, esto es: el empresario tiene la obligación de informar sobre la finalidad real del control de accesos y su capacidad sancionadora de forma previa, expresa, precisa, clara e inequívoca a los trabajadores, no pudiendo otorgar a la medida de control una fin distinto del que ya informó[245]; no es necesario el consentimiento del trabajador para que el empleador ejerza su poder de control[246]; el empresario debe poner en conocimiento de los representantes de los trabajadores la medida de control que pretende adoptar[247]; y, por último, el sistema de control biométrico ha de ser proporcional y estar debidamente justificado en un interés empresarial legítimo.

siquiera se trata de someter al sujeto a operaciones que le afecten físicamente, fuera del momento de recepción de la huella (…) por tanto entiende el juzgador, que se han cumplido todos los controles y las garantías precisas para salvaguardar el derecho fundamental a la intimidad y a la privacidad".

[244] En este sentido se ha pronunciado el Consejo de Ministros de la Unión Europea indicando que el control biométrico únicamente debe ser empleado cuando resulte totalmente necesario para los intereses del empresario, de los trabajadores o de terceros, y siempre que no existan medios menos intrusivos que permitan el cumplimiento de la finalidad buscada con el sistema biométrico, en su recomendación CM/Rec(2015)5. Disponible en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a (última visita: 01/07/2019).

[245] Según el TEDH, el deber informativo en relación con las medidas de control que pudiera adoptar el empresario para la vigilancia de sus trabajadores deberá ser ejercitado de manera rigurosa con tal de cumplir con la obligación informativa que el RGPD recoge en los artículos 13 y 14 y con los derechos de los trabajadores conocidos como "ARCO" (comprendidos en los artículos 15 – 21 RGPD y 13 – 18 LOPDGDD).

[246] Artículo 6.1.b) RGPD.

[247] Véase la STS de 19 de diciembre de 2005 (EDJ 250647) y el artículo 64.5.f) ET.

Que la medida de control sea proporcional quiere decir que los sistemas biométricos deben ser idóneos (en el caso de los lectores de huellas dactilares, estos deberán ajustarse al fin buscado por el empresario: la vigilancia del cumplimiento de las obligaciones laborales por parte de los trabajadores), necesarios (no debe existir otro medio, que permita el control de asistencia de los trabajadores, menos agresivo respecto a los DDFF de los trabajadores que cumpla con la finalidad de vigilancia) y proporcionales en sentido estricto (las ventajas que se deriven del uso del lector de huella dactilar deben ser mayores para el interés general que los inconvenientes que este tipo de control pudiera conllevar)[248]. Si la medida empresarial no cumple con estos requisitos, será considerada como ilícita por vulnerar los DDFF de los trabajadores, no pudiendo ser empleada en ningún caso.

Asimismo, por aplicación del RGPD, el empleo de técnicas biométricas de control requiere al empresario realizar las pertinentes evaluaciones de impacto, dada la especial naturaleza de este tipo de datos. Las evaluaciones de impacto sirven para determinar las medidas de seguridad que necesita una empresa para llevar a cabo el tratamiento de datos con las máximas garantías para los afectados (en este caso, los trabajadores). Durante el desarrollo de las evaluaciones, también se verifica que el sistema biométrico cumpla con el triple juicio de proporcionalidad tal y como se ha visto. En consecuencia, las evaluaciones de impacto resultan un elemento clave para la posterior implantación de medidas de control biométricas, dado que permite al empresario conocer de manera previa los posibles riesgos que la instalación de un lector de huella dactilar va a comportar[249].

En definitiva, el control de accesos a través de sistemas biométricos y las pruebas que puedan resultar de su ejercicio serán lícitos, cuando no existan medios menos invasivos para los derechos de los trabajadores capaces de cumplir con el mismo fin, cuando el empresario cumpla con su deber informativo con sus empleados y los representantes legales de estos, y cuando la técnica de control sea proporcional según el establece el TC.

---

[248] En este sentido, véanse los artículos 5.1 y 6 RGPD. Sobre el test de proporcionalidad, véase también BLÁZQUEZ AGUDO, E. M., *Aplicación práctica de la… Op. Cit.*, págs. 41 – 44; así como las SSTC 96/2012, de 7 de mayo; 55/1996, de 28 de marzo, FJ 6º – 9º; 207/1996, de 16 de diciembre, FJ 4º; 66/1995, de 8 de mayo, FJ 5º; y 37/1998, de 17 de febrero, FJ 8º.

[249] Artículo 35 RGPD. Véase la Guía Práctica sobre la "Evaluación de impacto relativa a la protección de datos" elaborada por la Agencia Catalana de Protección de Datos (ADPCAT). Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-EVALUACION-DE-IMPACTO-CAST-2.0.pdf (última visita: 10/07/2019).

CONCLUSIONES

I.- El impacto de las NTIC en las organizaciones

La aplicación de las NTIC al mundo empresarial ha supuesto importantes cambios organizativos. El uso de nuevas tecnologías contribuye a una mayor confusión entre la vida privada y la vida profesional del trabajador, por lo que su empleo en las RRLL ha propiciado el surgimiento de nuevos conflictos, en este sentido. Esta generalización tecnológica ha puesto de manifiesto la necesidad de determinar qué derechos y obligaciones entra en juego en relación con el uso de NTIC en el ámbito laboral.

II.- La reciente normativa en materia de protección de datos

Nos encontramos en un periodo de adaptación a la reciente regulación en materia de protección de datos: el RGPD y la LOPDGDD. Dichas normas incluyen diversos preceptos relativos a los derechos digitales de los trabajadores como: la desconexión digital, la protección de la intimidad en el uso de las NTIC y frente al control empresarial ejercido a través de la videovigilancia, la geolocalización, y la grabación de sonidos de los trabajadores.

La falta de normativa específica que existía sobre el empleo de la tecnología en el marco laboral ha venido provocando que sean los tribunales los encargados de dirimir los conflictos en este sentido. La jurisprudencia no ha sido uniforme en cuanto a determinar qué condiciones son necesarias para determinar la licitud de la medida de control empresarial, si bien recientes sentencias del TEDH han marcado el camino a seguir.

III.- El poder de control del empresario

Las facultades empresariales de dirección, control y disciplina no son absolutas. Por lo que pueden verse limitadas por el debido respeto a la dignidad del trabajador, el deber de buena fe contractual y los DDFF de los trabajadores. Por lo que la principal incógnita versa sobre cuáles son las condiciones que la actuación empresarial debe cumplir para afirmar que su uso no lesiona ningún DDFF y es, por tanto, lícito.

IV.- Los DDFF de los trabajadores: intimidad, secreto de las comunicaciones y protección de datos de carácter personal

Los DDFF protegen a todos los ciudadanos, por lo que también operan en el marco de una relación jurídico laboral. No obstante, estos derechos admiten ciertas limitaciones como consecuencia de la confrontación con otros derechos constitucionalmente protegidos (como es el interés empresarial). En atención al uso de NTIC en el ámbito laboral, cobran especial relevancia los DDFF relativos a la intimidad, al secreto de las comunicaciones, y a la protección de datos.

Los trabajadores pueden ejercer su derecho a la intimidad durante la prestación laboral, de manera que, de su confrontación con el poder de control empresarial surgen dos importantes cuestiones a resolver: el uso personal o laboral que el empleado da a las herramientas de trabajo puestas a disposición por el empresario; y la necesidad de establecer límites a la vigilancia empresarial para no lesionar este derecho.

El control de las conversaciones de los trabajadores puede afectar tanto al derecho al secreto de las comunicaciones como al derecho a la intimidad. En este sentido, si el contenido del mensaje hace referencia a la vida personal de los comunicantes, su difusión podría lesionar el derecho a la intimidad.

El derecho a la protección de datos de carácter personal conlleva para el empresario la obligación de informar sobre la medida de control aplicada en la empresa. El deber informativo es un complemento indispensable para el derecho a la protección de datos que debe ejercitarse de forma previa, expresa, precisa, clara e inequívoca a los trabajadores, sobre la finalidad del control de la actividad laboral.

En el ámbito de las RRLL, no es necesario que el trabajador dé su consentimiento expreso para el uso de sus datos personales, pues el vínculo contractual supone una autorización tácita en este sentido. No obstante, en el caso de los derechos a la intimidad y al secreto de las comunicaciones, la autorización previa por parte del trabajador ejerce de límite a estos DDFF.

V.- La prueba prohibida en el proceso laboral

Los dispositivos digitales permiten dejar constancia de posibles irregularidades de los trabajadores, convirtiéndose así en un medio de prueba capaz de acreditar sanciones disciplinarias. Si las medidas de control empresarial vulneran los DDFF de los

trabajadores, el resultado de su ejercicio (elementos de prueba) serán ilícitos y no podrán aportarse ni practicarse en un proceso judicial.

En este sentido, la doctrina de la prueba lícita establece que no surtirán efecto las pruebas obtenidas, directa o indirectamente, vulnerando los DDFF (artículo 11.1 LOPJ). Esta regla de exclusión probatoria contiene, asimismo, el llamado efecto reflejo de las pruebas prohibidas, según el cual, los elementos probatorios que se deriven de otros obtenidos lesionando DDFF, serán igualmente ilícitos e inadmisibles en un proceso judicial.

No obstante, la jurisprudencia ha venido admitiendo una serie de excepciones a la doctrina de la prueba ilícita y al efecto reflejo de la prueba prohibida con el fin de evitar que la absolución de investigados cuando la acusación se fundamenta en pruebas obtenidas, directa o indirectamente, lesionando DDFF.

Asimismo, cabe la limitación de los DDFF de los trabajadores si la medida empresarial que los lesiona supera dos condiciones, estas son: que el control empresarial esté debidamente justificado y que supere el test de proporcionalidad (que la mediada sea idónea, necesaria y equilibrada). Sin embargo, habrá que valorar la circunstancias de cada caso, pues según el DDFF afectado podrán exigirse requisitos adicionales.

VI.- Medidas empresariales que afectan al derecho a la intimidad de los trabajadores

Para valorar si una medida empresarial transgrede el derecho a la intimidad de los trabajadores, la misma deberá estar debidamente justificada y superar el test de proporcionalidad, atendiendo a las circunstancias de cada caso (como el lugar de la instalación, si la medida es puntual o permanente, si el dispositivo tecnológico está oculto, o si los trabajadores y/o sus representantes conocen la medida).

El triple examen de proporcionalidad se centra en ponderar los intereses de ambas partes de una relación laboral aplicando un triple juicio: idoneidad (la medida ha de ser capaz de cumplir con el objetivo empresarial); necesidad (no debe existir un medio menos restrictivo de los DDFF de los trabajadores que cumpla con el fin empresarial); proporcionalidad en sentido estricto (de la aplicación de la medida deben derivan más beneficios que desventajas). La no superación de cualquiera de estas condiciones supondrá la ilicitud de la medida, así como la prohibición de las pruebas obtenidas como resultado del control empresarial ilegítimo.

VII.- Medidas empresariales que afectan al derecho a la protección de datos de carácter personal de los trabajadores

Si la medida empresarial supone un tratamiento de los datos personales del empleado (datos de geolocalización, huellas dactilares, imágenes, y/o sonidos), el empresario debe informar a los trabajadores y/o representantes de forma previa, expresa, clara e inequívoca sobre los medios de control a adoptar, así como la finalidad de estos, no pudiendo otorgar a la medida de control una fin distinto del que ya informó. La falta de información conculca el artículo 18.4 CE y genera una "expectativa razonable de confidencialidad" en los trabajadores.

La colocación en el centro de trabajo de un distintivo señalizando la existencia de cámaras no es suficiente para dar por cumplida la obligación de informar -a pesar de así quede contemplado en la LOPDGDD- pues los medios de control subrepticios vulneran el artículo 8 CEDH.

Asimismo, los medios de control que afecten al derecho contenido en el artículo 18.4 CE, deberán justificarse en un interés legítimo y superar el test de proporcionalidad para ser lícitos.

VIII.- El control audiovisual de los trabajadores

Se permite el control de actividad laboral a través de grabación de sonidos y/o imágenes; no obstante, el uso simultáneo de ambos medios resulta especialmente invasivo para la intimidad de los trabajadores. Asimismo, existen determinados lugares situados dentro del centro de trabajo -vestuarios, comedor, zonas de descanso o esparcimiento- en los que no está permitido el control audiovisual.

IX.- Control de los trabajadores a través de detectives privados

La jurisprudencia permite el control de los trabajadores más allá del lugar y horario de trabajo a través de detectives privados, siempre que la conducta del trabajador afecte a la empresa y pueda suponer una transgresión de la buena fe contractual.

Sin embargo, los detectives no pueden investigar sobre la vida íntima de los trabajadores; si bien, podrán obtener datos referentes a su vida personal, laboral y familiar, en tanto en cuanto esta información se ciñe a la esfera de la vida privada de las personas. Del mismo modo, queda prohibida la captación de imágenes y/o sonidos en lugares privados, salvo autorización expresa del propietario; no obstante, si la conducta

que el detective investiga puede ser percibida desde una zona pública, su testimonio resultará válido como prueba en un proceso.

La regulación en materia de protección de datos en el marco de la investigación privada es más difusa que en lo referente a otros medios tecnológicos de control, por lo que resulta de gran importancia adaptar la LSP a tiempos actuales. Asimismo, existen criterios diversos sobre la aplicación de la tutela informativa a la investigación privada; si bien el TEDH no hace referencia a este aspecto, en cumplimiento de su doctrina, habrá que acatar la exigencia del deber informativo de igual forma que el resto de sistemas de control empresarial.

X.- Control sobre las herramientas informáticas puestas a disposición por la empresa

El empresario puede entregar al trabajador elementos informáticos que este use como herramientas para el desempeño de su actividad laboral. Las herramientas informáticas podrán ser controladas por el empresario en la medida en que estas le pertenecen.

En este sentido, no es necesario que el trabajador autorice la instalación de un dispositivo GPS en el coche de empresa o de un programa de control de la navegación en internet en su ordenador de la oficina; si bien, el deber de información deberá cumplirse en todo caso de forma previa, clara, expresa e inequívoca sobre la existencia del control y la finalidad sancionadora del mismo.

El empresario debe establecer una política de empresa donde permita, o no, el uso personal de las herramientas de trabajo. En caso de no existir un precepto expreso (ya sea por normativa, convenio colectivo o mandato empresarial) prohibiendo el uso personal, la jurisprudencia acepta el eventual uso privado -y moderado- de los dispositivos tecnológicos. Asimismo, la tipificación como sanción del uso particular de las herramientas puestas a disposición por el empresario en el Convenio Colectivo de aplicación, presupone la prohibición del uso particular y permite el control empresarial sobre el dispositivo.

XI.- Control biométrico

El RGPD clasifica los datos biométricos (huellas dactilares, iris, voz, etc.) como datos personales de categoría especial, por lo que su tratamiento queda prohibido, salvo

que el titular dé su consentimiento expreso a tal efecto o se trate de una relación laboral. El empleo de técnicas biométricas de control requiere, además, que el empresario realice las pertinentes evaluaciones de impacto.

BIBLIOGRAFÍA

ALFONSO MELLADO, C. L., "La prueba de detectives en el proceso laboral", en *Estudios sobre ciencia de seguridad: policía y seguridad del Estado* (Dir. ANTÓN BARBERÁ, F., y CERVELLÓ DONDERIS, V.), Tirant lo Blanch, Valencia, 2012.

APARICIO ALDANA, R. K., *Derecho a la intimidad y a la propia imagen en las relaciones jurídico laborales,* Thomson Reuters-Aranzadi, Cizur Menor, 2016.

ARIAS DOMÍNGUEZ, A.; RUBIO SÁNCHEZ, F., *El derecho de los trabajadores a la intimidad,* Aranzadi, Pamplona, 2006.

ARIAS DOMÍNGUEZ, A.; SEMPERE NAVARRO, A. V., *Detectives en las Relaciones Laborales. Impacto de la Ley de Seguridad Privada (L 5/2014),* Francis Lefebvre, Madrid, 2014

ARMENTA DEU, M. T., *La prueba ilícita (un estudio comparado),* Marcial Pons, Madrid, 2011.

ARRABAL PLATERO, P., "La videovigilancia laboral como prueba en el proceso", *Revista General de Derecho Procesal,* IUSTEL, núm. 37, 2015.

BLÁZQUEZ AGUDO, E. M., *Aplicación práctica de la protección de datos en las relaciones laborales,* Wolters Kluwer, Madrid, 2018.

DESDENTADO BONETE, A.; MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo,* Lex Nova, Valladolid, 2012.

DÍAZ RODRÍGUEZ, J. M., *Detectives y vigilantes privados en el ámbito laboral. Poder empresarial y prueba judicial*, Tirant lo Blanch, Valencia, 2013.

DOCTOR SÁNCHEZ-MIGALLÓN, R., "La vigilancia de la actividad del trabajador mediante videocámaras y circuitos cerrados de televisión", *IUSLabor*, núm. 3, 2014.

FERNÁNDEZ ESTEBAN, M. L., "Estudio de la jurisprudencia constitucional y ordinaria sobre el secreto de las telecomunicaciones entre particulares, en especial en el ámbito de la empresa", *Revista Aranzadi Doctrinal Civil-Mercantil*, núm. 3, 2000.

FUENTES SORIANO, O., "Videos, comunicación electrónica y redes sociales: cuestiones probatorias", *Práctica de Tribunales,* núm. 135, Wolters Kluwer, 2018.

GALIANA MORENO, J. M .; LUJÁN ALCARAZ, J ., "El proceso ordinario y otras modalidades procesales" en *Curso de procedimiento laboral* (MONTOYA MELGAR, A.; GALIANA MORENO, J. M.; SEMPERE NAVARRO, A. V.; RÍOS SALMERÓN, B.; CAVAS MARTÍNEZ, F.; LUJÁN ALCARAZ, J.), Tecnos, 2016.

GARBERÍ LLOBREGAT, J., *El nuevo proceso laboral*, Civitas, Madrid, 2011.

GARCÍA-PERROTE ESCARTÍN, I., "La prueba en el proceso de trabajo", *Relaciones Laborales,* núm. 12, 2001.

GARCÍA-PERROTE ESCARTÍN, I., "Prueba y Proceso Laboral", *Derecho Privado y Constitución*, núm. 4, 1994.

GIMENO SENDRA, V., *Introducción al Derecho Procesal,* Ediciones Jurídicas Castillo de Luna, Madrid, 2017.

GONZÁLEZ GONZÁLEZ, C., "Control empresarial de la actividad laboral mediante video vigilancia y colisión con los derechos fundamentales del trabajador. Novedades del Proyecto de Ley Orgánica de protección de datos derechos digitales", *Revista Aranzadi Doctrinal*, núm.4, 2019.

GOÑI SEIN, J.L., *La videovigilancia empresarial y la protección de datos personales*, Civitas, Madrid, 2017.

GOÑI SEIN, J.L., "Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?, en *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social: XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social* (VVAA), Ediciones Cinca, Pamplona, 2014.

GUDE FERNÁNDEZ, A., "La videovigilancia laboral y el derecho a la protección de datos de carácter personal", *Revista de Derecho Político*, set-dic 2014, núm. 91.

LLAMOSAS TRAPAGA, A., *Relaciones laborales y nuevas tecnologías de la información y la comunicación,* Dykinson, Madrid, 2015.

LÓPEZ ORTEGA, J. J., "La utilización de medios técnicos de observación", *La protección jurídica de la intimidad*, IUSTEL, Valencia, 2010.

LÓPEZ PEÑA, A., *Innovación tecnológica y cualificación (La polarización de las cualificaciones de la empresa)*, CES, Madrid, 1996.

MIRANDA ESTRAMPES, M., "La prueba ilícita: la regla de exclusión probatoria y sus excepciones", *Revista Catalana de Seguretat Pública*, núm. mayo 2010.

MONTOYA MELGAR, A., "El poder de dirección del empresario en las estructuras empresariales complejas", *Revista del Ministerio de Trabajo y Asuntos Exteriores*, núm. 48, 2004.

PALOMEQUE LÓPEZ, M. C., *Los derechos laborales en la Constitución Española*, CES, Madrid, 1991.

PUJOLAR, O., "Poder de dirección del empresario y nuevas formas de organización y gestión del trabajo", *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 2, 2005.

RODRÍGUEZ ESCANCIANO, S., *Poder de Control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, Valencia, 2015.

RODRÍGUEZ LAINZ, J. L., "Análisis del espectro electromagnético de señales Inalámbricas: rastreo de dispositivos wi-fi", *Diario La Ley*, núm. 8588, 2015.

ROMÁN DE LA TORRE, M. D., *Poder de dirección y contrato de trabajo*, Grapheus, Valladolid, 1993.

ROQUETA BUJ, R., "El derecho a la intimidad de los trabajadores", *Protección jurídica de la intimidad*, IUSTEL, Madrid, 2012.

SALGADO SEGUÍN, V., "Intimidad, privacidad y honor en internet", *TELOS 85: Los derechos fundamentales en internet*, TELOS: Cuadernos de Comunicación e Innovación, Madrid, 2010.

SAN MARTÍN MAZZUCCONI, C.; SEMPERE NAVARRO, A. V., *Las TICs en el ámbito laboral*, Francis Lefebvre, Madrid, 2015.

VILLAVERDE MENÉNDEZ, I., "La Jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos" en *La protección de datos de carácter personal en los centros de trabajo* (Dir. FARRIOLS I SOLÀ, A.), Ediciones Cinca, Madrid, 2006.

WEBGRAFÍA

- Noticia "Nomofobia: esclavos del móvil", publicada por Paz Olivares Sánchez en Efesalud. Disponible en: https://www.efesalud.com/nomofobia-esclavos-del-movil/

- "Informe ditrendia: Mobile en España y en el Mundo 2018", elaborado por Ditrendia en colaboración con la Asociación de Marketing de España (MKT) y Mobile Marketing Association (MMA). Disponible en: https://mktefa.ditrendia.es/hubfs/Ditrendia-Informe%20Mobile%202018.pdf?t=1532079210754&utm_campaign=Informe%20Mobile%202018&utm_source=hs_automation&utm_medium=email&utm_content=64334773&_hsenc=p2ANqtz--cx3JSF8KsY23QL5n_hdEfexpA53INssRdwpW2vGb0GDM4dsTbTyo

- "Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del comercio electrónico en las empresas", elaborada por el Instituto Nacional de Estadística (INE). Disponible en: https://www.ine.es/prensa/tic_e_2017_2018.pdf

- Ponencia "Las prestaciones de servicios a través de las plataformas digitales: un nuevo desafío para el Derecho del Trabajo", de CAVAS MARTÍNEZ, F., realizada en el marco del III Seminario del área de Derecho del Trabajo y de la Seguridad Social, celebrado el 1 de marzo de 2017 en la Universidad Miguel Hernández de Elche (Alicante). Disponible en: https://youtu.be/RK1-B1yd5gs

- Artículo "Las consecuencias laborales y sociales del avance de las nuevas tecnologías en el mundo empresarial", publicado en el blog del bufete de abogados Casadeley. Disponible en: https://www.bufetecasadeley.com/consecuencias-laborales-tecnologia-empresas/

- Artículo "La prueba digital en el procedimiento laboral", publicado por el abogado Pere Vidal López en el Blog Laboral de LegalToday. Disponible en: http://www.legaltoday.com/practica-juridica/social-laboral/laboral/la-prueba-digital-en-el-procedimiento-laboral

- Entrada "Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral", publicada por Alexandra Garcés en el blog de la firma de abogados ECIJA. Disponible en: https://ecija.com/derecho-a-la-intimidad-ante-la-utilizacion-de-sistemas-de-geolocalizacion-en-el-ambito-laboral/

- Ponencia "Los Derechos y Libertades Fundamentales en materia laboral", de CAVAS MARTÍNEZ, F., realizada en el marco del I Seminario del Área de Derecho del Trabajo y la Seguridad Social, el 23 de febrero de 2015 en la Universidad Miguel Hernández de Elche (Alicante). Disponible en: https://youtu.be/fECK5u0FO6A

- Entrada "La Constitución Española y su contenido laboral", publicada por FERNÁNDEZ GARCÍA, A., en su blog "AFlabor". Disponible en: https://aflabor.wordpress.com/2012/12/11/la-constitucion-espanola-y-su-contenido-laboral/

- Sinopsis del artículo 18 CE, elaborada por ELVIRA PERALES, A., y actualizada por la Letrada de las Cortes Generales Ángeles González Escudero. Disponible en: http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2

- Informe jurídico núm. 0240/2009 de la AEPD. Disponible en: https://www.aepd.es/informes/historicos/2009-0240.pdf

- Diccionario del español jurídico de la Real Academia Española. Disponible en: https://dej.rae.es

- Seminario "El proceso y la prueba", cuyas ponentes son LÓPEZ YAGÜES, V., FUENTES SORIANO, O., y FERNÁNDEZ LÓPEZ, M., celebrado el 24 de mayo de 2018 en la Universidad Miguel Hernández de Elche. Disponible en: https://youtu.be/ifZQPrRIzck

- Entrada "La prueba digital en el ámbito laboral ¿son válidos los pantallazos?", publicada por Raúl Rojas Rosco en su blog "Laboral 3.0". Disponible en: http://raulrojas.es/234-2/

- Informe Jurídico núm. 0006/2009 de la AEPD. Disponible en: https://www.aepd.es/informes/historicos/2009-0006.pdf

- Ficha práctica de videovigilancia de la AEPD sobre información general. Disponible en: https://www.aepd.es/media/fichas/ficha-videovigilancia-folleto-general.pdf

- Ficha práctica sobre videovigilancia y control empresarial de la AEPD. Disponible en: https://www.aepd.es/media/fichas/ficha-videovigilancia-control-empresarial.pdf

- Distintivo "Zona Videovigilada" exigido por la AEPD. Disponible en: https://www.aepd.es/media/fichas/cartel-videovigilancia.pdf

- "Guía para el cumplimiento del deber de informar", elaborada por la AEPD en colaboración con las Agencias de Protección de Datos del País Vasco y Cataluña. Disponible en: https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

- "Anuario y Estadísticas. Habilitaciones de personal de Seguridad Privada", elaborada por el Ministerio del Interior del Gobierno de España. Disponible en: http://www.interior.gob.es/ca/web/archivos-y-documentacion/seguridad-privada4

- VII Informe Adecco sobre Absentismo, elaborado por The Adecco Group. Disponible en: https://www.adeccogroup.es/wp-content/uploads/2018/06/VII-Informe-Adecco-sobre-Absentismo-Laboral.pdf

- Noticia "Las bajas fraudulentas ya copan el 90% del trabajo de los detectives privados", publicada en la edición digital del periódico El País. Disponible en: https://cincodias.elpais.com/cincodias/2018/10/09/fortunas/1539108545_471618.html

- Tabla de "indicadores sobre el uso de TIC en las empresas – Año 2017 y T1 2018", elaborada por el Instituto Nacional de Estadística (INE). Disponible en: https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176743&menu=ultiDatos&idp=1254735576799

- Informe Jurídico núm. 0242/2008 de la AEPD, sobre el control del trabajador a partir del filtrado de correos electrónicos. Disponible en: https://www.aepd.es/informes/historicos/2008-0242.pdf

- Recomendación CM/Rec(2015)5, del Consejo de Ministros de la Unión Europea. Disponible en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

- Entrada "Control empresarial y Geolocalización", realizada por PURCALLA BONILLA, M. A., en el blog de FERNÁNDEZ GARCÍA, A., "AFlabor". Disponible en: https://aflabor.wordpress.com/2017/07/21/control-empresarial-y-geolocalizacion-colaboracion-de-miquel-angel-purcalla-bonilla/

- Informe Jurídico núm. 0090/2009 de la AEPD, sobre la proporcionalidad en el tratamiento de los datos de localización. Disponible en: https://www.aepd.es/informes/historicos/2009-0090.pdf

- Informe Jurídico núm. 0193/2008 de la AEPD. Disponible en: https://www.aepd.es/informes/historicos/2008-0193.pdf

- Guía "Tecnologías biométricas aplicadas a la ciberseguridad" elaborada por el Instituto Nacional de Seguridad (INCIBE). Disponible en: https://www.incibe.es/protege-tu-empresa/guias/tecnologias-biometricas-aplicadas-ciberseguridad-guia-aproximacion-el

- Guía Práctica sobre la "Evaluación de impacto relativa a la protección de datos", elaborada por la Agencia Catalana de Protección de Datos (ADPCAT). Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-EVALUACION-DE-IMPACTO-CAST-2.0.pdf

ÍNDICE JURISPRUDENCIAL

EPÍGRAFE I.- EL CONTROL EMPRESARIAL SOBRE LA ACTIVIDAD LABORAL

1.- LOS PODERES DEL EMPRESARIO: DIRECCIÓN, CONTROL Y DISCIPLINA

- STC 96/2013, de 23 de abril.
- STC 96/2002, de 25 de abril.
- STC 225/1993, de 8 de julio.
- STC 88/1985, de 19 de julio.

2.- LOS LÍMITES AL EJERCICIO DEL PODER DE CONTROL EMPRESARIAL

- STS 479/2009, de 15 de junio.
- STC 236/2007, de 7 de noviembre.
- STC 70/2002, de 3 de abril.
- STSJ Cataluña 8041/2001, de 22 de octubre.
- STC 98/2000, de 11 de abril.
- STC 143/1994, de 9 de mayo.
- STC 57/1994, de 28 de febrero.
- STC 88/1985, de 19 de julio.

2.1.- Los Derechos Fundamentales como límite al control empresarial

- STC 88/1985, de 19 de julio.

2.1.1.- El Derecho Fundamental a la intimidad personal y familiar

- STSJ Comunidad Valenciana 567/2012, de 24 de febrero.
- STSJ Canarias 97/2011, de 3 de marzo.
- STC 70/2009, de 23 de marzo.
- STS de 26 de septiembre de 2007 (núm. rec. 966/2006).
- STC 186/2000, de 10 de julio.
- STC 202/1999, de 8 de noviembre.
- STC 134/1999, de 15 de julio.
- STC 151/1997, de 29 de septiembre.

- STC 143/1994, de 9 de mayo.
- STC 57/1994, de 28 de febrero.
- STC 231/1988, de 2 de diciembre.

2.1.2.- El Derecho Fundamental al secreto de las comunicaciones

- STS 678/2014, de 20 de noviembre.
- STC 281/2006, de 9 de octubre.
- STC 123/2002, de 20 de mayo.
- STC 114/1984, de 29 de noviembre.
- STEDH 1984\1, de 2 de agosto, en el asunto Malone contra el Reino Unido.

2.1.3.- El Derecho Fundamental a la protección de datos

- STC 170/2013, de 7 de octubre.
- STC 241/2012, de 17 de diciembre.
- STC 292/2000, de 30 de noviembre.
- STC 290/2000, de 30 de noviembre.
- STC 94/1998, de 4 de mayo.

2.2.- La prueba prohibida en el proceso laboral

- STSJ Canarias 19/2016, de 22 de enero.
- STSJ Cantabria 843/2015, de 10 de noviembre.
- STSJ Cataluña 3980/2015, de 17 de junio.
- STS 300/2015, de 19 de mayo
- STS de 2 de diciembre de 2014 (núm. rec. 97/2013).
- STC 29/2013, de 11 de febrero.
- STC 96/2012, de 7 de mayo.
- STSJ Cataluña 1197/2012, de 14 de febrero.
- STC 66/2009, de 9 de marzo.
- STS 636/2008, de 2 de octubre.
- STC 261/2005, de 24 de octubre.
- STC 22/2003, de 10 de febrero.

- STC 28/2002, de 11 de febrero.
- STC 308/2000, de 18 de diciembre.
- STC 136/2000, de 10 de julio.
- STC 98/2000, de 10 de abril.
- STC 50/2000, de 28 de febrero.
- STC 49/1999, de 5 de abril.
- STC 81/1998, de 2 de abril.
- STC 37/1998, de 17 de febrero.
- STC 1/1998, de 12 de enero.
- STC 207/1996, de 16 de diciembre.
- STC 49/1996, de 26 de marzo.
- STC 55/1996, de 28 de marzo.
- STC 181/1995, de 11 de diciembre.
- STC 86/1995, de 6 de junio.
- STC 66/1995, de 8 de mayo.
- STC 143/1994, de 9 de mayo.
- STC 99/1994, de 11 de abril.
- STC 85/1994, de 14 de marzo.
- STC 57/1994, de 28 de febrero.
- STC 80/1991, de 15 de abril.
- ATS de 18 de junio de 1992 (núm. rec. 610/1990).
- STC 64/1986, de 21 de mayo.
- STC 107/1985, de 7 de octubre.
- STC 114/1984, de 29 de noviembre.

EPÍGRAFE II.- LAS NUEVAS TECNOLOGÍAS COMO MEDIOS DE CONTROL EMPRESARIAL

1.- EL CONTROL AUDIOVISUAL DE LOS TRABAJADORES

- STC 29/2013, de 11 de febrero.
- STC 186/2000, de 10 de julio.
- STC 98/2000, de 10 de abril.

- STSJ Comunidad Valenciana 383/2000, de 3 de febrero.

1.1.- La grabación de audio de los trabajadores

- STC 98/2000, de 10 de abril
- STSJ Madrid 412/2006, de 14 de junio.
- STSJ Cataluña de 24 de abril de 2007.
- STS, sala de lo Social, de 5 de diciembre de 2003 (núm. rec. 52/2003).
- STSJ Murcia 162/2003, de 3 de febrero.
- STC 202/1999, de 8 de noviembre.
- STC 142/1993, de 22 de abril.
- STC 180/1987, de 12 de noviembre.
- STC 207/1996, de 16 de diciembre;
- STC 55/1996, de 28 de marzo.
- STC 66/1995, de 8 de mayo.

1.2.- La videovigilancia de los trabajadores

- Sentencia del Juzgado de lo Social núm. 3 de Pamplona 52/2019, de 18 de febrero.
- STEDH, de 9 de enero de 2018, en el asunto López Ribalda y otras v. España.
- STS de 2 de febrero de 2017.
- STS de 31 de enero de 2017.
- STS 7 de julio de 2016.
- STC 39/2016, de 3 de marzo.
- Sentencia del Juzgado de lo Social núm. 3 de Elche, de 14 de mayo de 2014.
- STS de 13 de mayo de 2014 (núm. rec. 1685/2013).
- Sentencia del Juzgado de lo Social núm. 1 de Granollers, de 28 de enero de 2010.
- STSJ Cataluña de 11 de marzo de 2013.
- STC 29/2013, de 11 de febrero.
- STSJ Cataluña 1481/2011, de 24 de febrero.
- STSJ Madrid de 14 de abril de 2009.
- ATS 28/2007, de 11 de enero.
- STSJ Castilla y León 1479/2006, de 18 de septiembre.
- STSJ Madrid 2155/2000, de 14 de septiembre.

- STC 98/2000, de 10 de abril.
- STC 186/2000, de 10 de julio.
- STC 292/2000, de 30 de noviembre.

1.3.- Los detectives privados en el ámbito laboral

- STS 528/2017, de 20 de junio.
- STSJ Canarias 232/2017, de 27 de marzo.
- STS de 15 de octubre de 2014 (núm. rec. 1654/2013).
- STSJ Madrid 915/2010, de 5 de noviembre.
- STC 283/2000, de 27 de noviembre.
- STSJ Comunidad Valenciana 383/2000, de 3 de febrero.
- STS de 6 de noviembre de 1990 (núm. rec. 93/1990).

2.- LA MONITORIZACIÓN DEL ORDENADOR DE LOS TRABAJADORES

- STS 119/2018, de 8 de febrero.
- Sentencia del Juzgado de lo Social núm. 17 de Madrid, de 17 de noviembre de 2017.
- STEDH, de 5 de septiembre de 2017, en el asunto *Bârbulescu* v. Rumanía II.
- STC 170/2013, de 7 de octubre.
- STC 241/2012, de 17 de diciembre.
- STSJ Cantabria de 13 de noviembre de 2012 (EDJ 130230).
- STC 96/2012, de 7 de mayo.
- STS de 6 de octubre de 2011 (núm. rec. 4053/2010).
- STSJ Madrid 453/2011, de 30 de mayo.
- STSJ Madrid, 346/2011, de 28 de abril.
- STS de 8 de marzo de 2011 (núm. rec. 1826/2010).
- STSJ Cantabria 546/2009, de 24 de junio.
- STS 26 de septiembre de 2007 (núm. rec. 966/2006).
- STSJ País Vasco, de 21 de diciembre de 2004 (EDJ 254091).
- STSJ Castilla y León 512/2004, de 29 de marzo.
- STSJ Cantabria de 1 de marzo de 2004 (EDJ 40113).
- STSJ Cataluña de 15 de octubre de 2003 (núm. rec. 3637/2003).
- STSJ Cataluña 1506/2003, de 5 de marzo.

- STSJ Madrid 22 de noviembre de 2002 (núm. rec. 3806/02).
- STSJ Galicia 4168/2001, de 4 de octubre.
- STC 37/1998, de 17 de febrero.
- STC 207/1996, de 16 de diciembre.
- STC 55/1996, de 28 de marzo.
- STC 66/1995, de 8 de mayo.

3.- LA GEOLOCALIZACION DE LOS TRABAJADORES

- Resolución de la AN de 6 de febrero de 2019.
- STSJ Asturias, de 16 de noviembre de 2017.
- STC 39/2016, de 3 de marzo.
- STSJ Andalucía, de 15 de julio de 2015.
- STSJ Madrid, de 21 de marzo de 2014.
- STS de 21 de junio de 2012.
- STC 96/2012, de 7 de mayo.
- STSJ País Vasco, de 2 de junio de 2007.
- STC 207/1996, de 16 de diciembre.
- STC 55/1996, de 28 de marzo.
- STC 37/1998, de 17 de febrero.
- STC 66/1995, de 8 de mayo.

4.- EL CONTROL BIOMÉTRICO DE LOS TRABAJADORES

- SSTC 96/2012, de 7 de mayo.
- STSJ Andalucía 874/2007, de 3 de diciembre.
- STS de 2 de julio de 2007 (núm. rec. 5017/2003).
- STS de 19 de diciembre de 2005 (EDJ 250647).
- STSJ 28 de marzo de 2003 (núm. rec.759/02).
- STSJ Cantabria, de 10 de enero de 2003 (núm. rec. 517/02).
- STC 37/1998, de 17 de febrero.
- STC 207/1996, de 16 de diciembre.
- STC 55/1996, de 28 de marzo.
- STC 66/1995, de 8 de mayo.